Anti Money Laundering Exam Study Guide & Practice Exam

Enhance your studies for the ACAMS® CAMS exam with help from AML Expert

Comprehensive, plain-English revision notes
All key concepts included
88 question practice exam
Fully explained answers

Digitized by the Internet Archive
in 2023 with funding from
Kahle/Austin Foundation

https://archive.org/details/antimoneylaunder0000amle

If you obtained this document without making a contribution, please consider a donation towards the costs of providing this material at http://aml-expert.com/download.html

Study support materials that go along with this publication are available from http://www.aml-expert.com

We would like to wish you the very best of luck with your studies.

The contents of this study guide are subject to copyright.

© 2016 AML-expert.com.

Image Credit © 2009 K H Rawlings:
https://www.flickr.com/photos/khrawlings/

Licence: https://creativecommons.org/licenses/by/2.0/

No part of this guide may be reproduced in any form, including by photocopying or electronic means.

ACAMS® is a registered trademark of the Association of Certified Anti Money Launderers; this guide is not connected with them in any way.

Contents

Risks & Methods of Money Laundering and Terrorist Financing 6

Classic Money Laundering Process 7

Effects of Money Laundering 8

Money laundering techniques 9

Electronic transfers 9

Correspondent banking 9

Payable Through Accounts (PTAs) 10

Concentration Accounts 11

Private Banking 11

Structuring/Smurfing 12

Microstructuring 13

Cuckoo Smurfing 13

Bank Complicity 14

Credit Unions/Building Societies 14

Credit Cards 14

Money Remitters & Money Exchange Houses 14

Insurance Companies 15

Securities & Futures Broker-Dealers 16

Casinos & Gaming 16

Dealers in High Value Items 17

Travel Agencies 17

Vehicle Sellers 17

Gatekeepers: Accountants, Auditors, Lawyers, Notaries, Company Formation Agents 18

Investment and Commodity Advisors 18

Trust & Company Service Providers 19

Real Estate Industry 20

Reverse Flip 20
Loan back 20
Manipulation of import/export prices 20
Letters of Credit 21
Black Market Peso Exchange (BMPE) 21
Online/Internet Banking 21
Internet Casinos 22
Prepaid Cards and E-cash 22
Structures Designed to Hide Beneficial Ownership 25
Shell Companies 25
Front Companies 25
Buying a company already owned by the criminal 26
Double invoicing 26
Trusts 26
Bearer Bonds, Securities & Cheques 27
Terrorist Financing 27
Informal Value Transfer Systems 28
Charities & Non-for-profits 28
Compliance Standards for AML and Combating Financing of Terrorism 29
40 Recommendations 30
Overview of the 40 recommendations 32
Key highlights of the 40 recommendations 35
Non-Cooperative Counties 37
Basel Committee on Banking Supervision 37
EU Directives on Money Laundering 40
First Directive 40
Second Directive 40
Third Directive 40
Regional FATF-Style Bodies and FATF Associate Members 41

Other AML initiatives 44
Other International Organizations 45
Key US Legislation and Regulation relevant to International Transactions 46
USA Patriot Act 46
OFAC: Office of Foreign Assets Control 48
Key Groups 49
Chronological AML Developments 53
Anti-Money Laundering Compliance Program 55
Assessing Risk and Developing a Risk Scoring Model 56
Levels of risk 56
Geographical Location 57
Products and Services Risk 58
The Elements of an AML Program 60
Compliance Culture 64
Customer Due Diligence 64
Account opening guidelines from Basel 2003 64
Name lists 65
Arabic Names 65
Know Your Employee 66
Suspicious/Unusual Transaction Monitoring and Reporting 66
Red Flags 68
Electronic AML Solutions 72
Conducting and responding to an investigation 73
Law enforcement investigations 73
Decision to prosecute the institution 74
Responding to a law enforcement investigation 74
Summonses and Subpoenas 74
Search Warrants 75

Orders to restrain or freeze accounts or assets 75
Dealing with Investigators and Prosecutors 76
Obtaining Counsel for the Investigation 76
Notices to Employees 76
Media Relations 76
Internal Investigations 77
Closing the Account 77
Conducting the Investigation 77
Documents 78
Interviewing Employees 78
Attorney-Client Issues 78
International Cooperation 79
Mutual Legal Assistance Treaties 79
Financial Intelligence Units 80
The Supervisory Channel 81
Study Questions 83
Section 1 83
Section 2 91
Section 3 97
Section 4 102
Answer Sheet 106
Answers 107

Chapter 1 - Introduction

Risks & Methods of Money Laundering and Terrorist Financing

Definition

The process of making dirty money (derived from criminal activity) look clean by disguising the link to the source of the funds. This can be by moving the money or changing its form.

Laundering is not just about cash, almost any medium can be used including financial and non-financial instruments.

Money laundering requires knowledge that the money is the proceeds of crime, however, knowledge could also be inferred from wilful blindness (deliberate avoidance of the facts).

Classic Money Laundering Process

Money laundering has three distinct stages that transform the dirty money into clean money. These are outlined in the following table.

Placement **P**	Taking dirty money and physically depositing it with a financial institution or using it to purchase an asset. This is the highest risk area for the criminal, and most policing efforts are focussed here. Examples: depositing cash in a financial institution, purchasing high value assets such as art, precious metals or stones, which can then be sold with payment made by bank transfer or cheque.
Layering **L**	This distances the dirty money from its source by a series of transactions designed to help anonymity and disguise the audit trail. In this way the source, ownership, and location of the funds is disguised. Examples: wiring funds from one account to another, converting cash into depositary instruments (money orders, travellers cheques etc.), buying and reselling high value goods or prepaid access or stored value items (like gift cards), investing in property or legitimate businesses, investing in stocks bonds or life insurance, using shell companies which disguise the beneficial owner.
Integration **I**	Placing clean money into the economy using an apparently normal business or personal transaction, so that criminals can add it to their wealth. By this stage separating illegal and legal wealth is very difficult.

Effects of Money Laundering

- Increased crime and corruption
- Undermine the legitimate private sector by undercutting their prices
- Weakening financial institutions, possibly to the point of collapse (BCCI, Barings Bank for example). Reputational risk of dealing with criminals, costs of investigations and fines
- Loss of control over monetary policy in smaller countries, as the size of money laundering transactions causes measurement errors. This can cause currency exchange rate and interest rate fluctuations
- Economic distortion, because money launderers are not interested in the economics of a transaction, they will put their money into schemes that offers privacy rather than economic benefit
- Loss of tax revenue, as the funds are disguised, so the collection of taxes is more difficult. This increases the burden of taxation on normal tax payers
- Risks to privatisation, as criminals can outbid legitimate purchasers, so key assets come under criminal control
- Reputation risk for the country
- Social costs e.g. treating drug addicts

Chapter 2 - Techniques

Money laundering techniques

Electronic transfers

Wires, ACH, ATMs and credit/debit cards. Indicators of money laundering include:

- Transactions to secrecy havens or high risk areas without justification
- Many small incoming transactions that are then sent out of the account in one bulk payment
- Funds activity that is repetitive, unexplained, or with unusual patterns

Correspondent banking

- This is where one bank (the correspondent) provides services to another bank (the respondent). Banks set up these correspondent relationships across the globe to provide services in jurisdictions where they have no physical presence. Large international banks have many thousands of correspondent banking relationships. The respondents obtain services such as: cash management (e.g. interest bearing accounts in a range of currencies), international wires, cheque clearing, payable through accounts, foreign exchange. Credit worthy banks can be offered credit products such as letters of credit or credit card account services.

- Correspondent banking is vulnerable for two reasons:
- The financial institution carries out transactions for the customers of another institution. This indirect relationship means the customers identity hasn't been verified by first-hand knowledge
- The volumes of transactions mean that it's not possible to know which transactions represent legitimate business and which are suspicious
- Additional risks:
    - Although the regulatory regime may be understood, the effectiveness over a specific respondent bank may be difficult to ascertain
    - The level of AML controls at the respondent can be assessed using standard questionnaires, however the effectiveness of the due diligence may be difficult to ascertain
    - Nesting of respondent banks means that the correspondent is further away from the actual customer
- Note that the USA Patriot Act enforced a number of provisions against correspondent banking – see separate section for details.

Payable Through Accounts (PTAs)

These are accounts, similar to respondent accounts, but where the respondent bank offers the service direct to their customers. This means that they could send a wire transfer without first clearing the transaction with the respondent. This means that the respondent's customers can directly control funds at the correspondent bank without oversight from the respondent.

The PTA account has a number of subaccounts that can be offered to customers such as individuals, commercial businesses, exchange houses, or other banks.

Aspects of PTAs that could impact AML efforts:

- PTAs with banks in offshore locations may have weak licensing or supervision
- PTAs where the CDD is performed only on the respondent, not the respondent's customers
- PTAs where the sub account holders can deposit and withdraw currency
- PTAs used by a subsidiary of a respondent bank, which can perform banking activity without direct supervision

Concentration Accounts

- Also known as special use, omnibus, settlement, suspense, intraday, sweep or collection accounts. They are internal accounts used to assist with the settlement and processing of customer transactions, often in conjunction with private banking, trust and custody accounts, funds transfers.
- They pose an AML threat if the customer identifying information is lost when the account is used, this loses the audit trail.

Good practices include:

- Require dual signatures on all general ledger entries
- Prevent direct customer access to concentration accounts
- Capture information in customer statements
- Prevent customer knowledge of concentration accounts
- Reconcile the accounts frequently, ensure segregation between the reconcilement and those that use the accounts on a day-to-day basis
- Resolve discrepancies timely
- Monitor for recurring customer names

Private Banking

- Offered to wealthy customers who seek confidentiality and personalised service. Often operates semi-autonomously to other parts of the bank, and is highly lucrative.

Key factors in private banking:

- High profitability
- Competition
- Powerful clientele
- Confidentiality and secrecy between client and banker
- Trust between client and banker
- Commission-based compensation
- Relationship managers that can become client advocates in order to protect their clients
- Often assets move overseas to corporations in secrecy havens.
- PICs (Private Investment Companies) are established by individuals to hold assets. They maintain confidentiality and are used for tax or trust related reasons. The secrecy laws of the offshore havens where PICs are located conceals the true identity of the beneficial owner.
- Sometimes PICs are created with nominee owners (who hold the title to the company for the benefit of unnamed owners) this can sometimes be protected by attorney-client privilege to prevent information about the beneficial owner from being obtained.
- Many private banks establish PICs for clients, often using a trust company in an offshore secrecy haven.
- PEPs (Politically Exposed Persons) are a further risk in Private Banking, as they may have access to the proceeds of bribes, extortion, and embezzlement.

Structuring/Smurfing

- Organising a transaction in such a way as to avoid triggering a reporting or record-keeping threshold. It is one of the most well-known money laundering methods, and is a crime in many countries. The people who perform this activity are known as runners or smurfs, employed by the launderers. They deposit small amounts of cash under the reporting threshold, or purchase monetary instruments (cashiers cheques) in amounts under the reporting threshold.

- A structurer may have 20 or more accounts open, some in false identities of dead people. Cash is supplied to the structurer by a money broker. The structurer deposits the cash in small quantities. The money broker then uses cheques drawn on the accounts to make payments for exports from the country where the structuring takes place to a different country (often linked to drug production).

Microstructuring

- This is the same as structuring, but for very small amounts, e.g. $800. The cash from the sale of drugs is deposited in one country and often withdrawn in a foreign country to pay for the supplies of the drugs.

It is very difficult to detect, but some signs might be:

- Using blank deposit slips rather than paying in book slips
- Frequent small cash deposits not consistent with usual business or personal activity
- Cash deposits followed quickly by ATM withdrawals in a high risk country

Cuckoo Smurfing

This requires an insider in a financial institution, often a money remitter or alternative remittance system.

The first step is when a customer provides money to an alternative remittance system for transfer to a bank account in a foreign country. Rather than sending the money to the destination, the insider advises an accomplice in the destination country of the bank account details of where the cash should have been sent.

The associate then deposits dirty cash into the unwitting customer's account, who believes that it is the international transfer they awaited. Then the alternative remitter provides the funds to the associate, who has swapped dirty money for clean money received from the remitter, which is supported by a genuine receipt.

The bank account used here is often innocent, but the cash deposit would be by a launderer, so retain CCTV footage.

Bank Complicity

Employees can pose a significant money laundering risk. Background screening for criminal history should be performed, as well as ongoing monitoring for any employees that may be performing criminal activities. Screening should include outsourced staff such as cleaners.

Credit Unions/Building Societies

Although a low risk due to their small size, and the difficulty of hiding large transactions, they are still vulnerable because they contain a large volume of cash transactions.

Credit Cards

Includes:

- Credit card associations such as MasterCard, Visa, American Express, Discover
- Issuing banks, which issue cards to customers
- Acquiring banks, which process transactions for merchants who accept credit cards
- Third-party processors, who have contracts with issuers and acquirers to provide transaction processing and other services
- Credit cards are often used in the layering or integration stages, as cash payments to cards are often restricted. Accounts are usually over-paid, creating a credit balance, which can be returned via a refund.

Money Remitters & Money Exchange Houses

- Money remitters move money for their customers, who often don't have access to traditional banking services; they are also often

cheaper than banks. Their services also cover all global locations, including ones without a formal banking infrastructure.

Key types:

- Separate networks such as Western Union and MoneyGram
- Underground networks (alternative remitters)
- Money transfers via foreign branches of a bank, where visiting workers can remit funds back home
- International money orders
- They can be well regulated, if properly licensed.

Insurance Companies

- Investment products such as life insurance, which can be cancelled and cashed in (whole of life or permanent life) and annuities are highest risk. Annuities allow a large cash payment to be exchanged for a series of income payments. This is similar to purchasing investments such as stocks, shares or bonds. Normal insurance (car, household etc.) do not have the redeemable value feature and are thus not susceptible to money laundering. Key risks:
- Brokers have a lot of freedom over the policies they sell
- Salesmen may not work for the insurance company, and be incentivised to sell, which makes them overlook suspicions
- Overpaying the insurance, and receiving the payment as a clean money cheque from the insurance company
- Using the 'free look' period to take out a policy, the cancel it without penalty for a clean cheque
- Redeeming polices early, paying the redemption charge, and receiving a clean cheque. Customers who are more interested in the cancellation terms than the policy may be a money launderer
- Products that allow purchase with cash or cash equivalents
- Products that allow a customer to borrow money against the product

Securities & Futures Broker-Dealers

- The industry runs on electronic transfers not cash, so is usually part of the integration or placement stages.

Key risk areas:

- High speed, international nature, using wire transfers
- Ease of converting to cash without loss or penalty
- Competitive, commission driven culture, meaning salespeople can overlook the source of funds
- Use of nominee or trustee accounts, obscuring true beneficiaries
- Use of cash trading accounts which are not subject to the AML controls of banks
- There are also activities within the securities markets, such as insider trading and market manipulation which generate illegal funds that need to be laundered.
- Wash trading is where two opposite transactions are placed – for example dirty money could be introduced into a brokerage, and a long and a short position could be taken on the same security or future in different brokerages. No matter which way the market moves, the principal is safe, as losses on one side are offset by gains on the other side. If the market moves so that the dirty money is lost, then the gains in the other brokerage account can be withdrawn which look like legitimate investment returns.

Casinos & Gaming

- Bookmakers, horseracing, and lotteries all are cash intensive, and offer a potential source of recently acquired wealth.
- Casino money laundering is usually at the placement stage, converting cash into cheques. The cash is used to buy chips, and then the chips can be converted into a cheque drawn on the casino's account. The credit can also be transferred to a different jurisdiction where the casino operates, and the funds can be made available there.

- One method of gambling is to bet in such a way as to risk very little of your capital (e.g. by betting on favourites). The winnings can then be withdrawn and are the verifiable winnings from gaming.

Dealers in High Value Items

- Precious metals, gem stones, jewellery, art and antiques are all vulnerable. Gold is compact, valuable, and convertible to cash in many parts of the world anonymously. For example, gold or diamonds can be purchased using cash generated from drug sales. The gold or diamonds can be smuggled back to the drug production country and converted into clean money. This then funds the drug production, with the reminder as profits for the producer. Often dealers will buy the high value item, and will make payment to a third party, allowing the change of the item from one form to another (e.g. object to cash) and from one person to another. As a result, this feature is useful in the layering phase.
- Art auction houses have very high value items which are bought by anonymous agents for elusive purchasers. The funds for the purchase arrive as a wire transfer from an off-shore location.

Travel Agencies

- Susceptible to money laundering where an expensive ticket or hotel package is purchased for another person, who then cancels and obtains a refund.

Vehicle Sellers

Cars and other vehicles (aircraft, helicopters, yachts) are susceptible to money laundering for four reasons:

- You can often make multiple part payments, allowing you to structure a cash deposit
- You can downgrade your vehicle, and accept the difference in a cheque made out to a third party (or yourself) which represents clean money, or a layering technique

- Dealers will accept third party payments for the vehicle (layering technique)
- The ability to trade multiple vehicles, which creates complex layers of transactions

Gatekeepers: Accountants, Auditors, Lawyers, Notaries, Company Formation Agents

- They can all facilitate the entry of illicit money into the financial system via the following methods:
- Creating corporate vehicles and complex legal entities such as trusts. These obscure the links between the proceeds of crime and the perpetrator
- Buying and selling property can be used in the layering stage, or in the integration stage where the asset is purchased and retained
- Performing financial transactions on behalf of a client (making deposits, issuing cheques, making and receiving wires, buying and selling stock)
- Providing financial and tax advice. Criminals may pose as wealthy individuals who need help sheltering wealth from tax.
- The issue of lawyers or attorneys providing advice to their client is controversial, as they have a confidential relationship with their clients.

Investment and Commodity Advisors

- Accounts for commodities futures and options can be used for laundering. These include:
- Commodities: food, grains and metals are traded on exchanges, often using futures
- Commodity pools: combines funds from several members to allow them to trade
- Futures: contracts to buy or sell a commodity at a future date and set price

- Omnibus accounts: accounts held at a futures merchant on behalf of another merchant, the transactions for multiple customers are combined which obscures their identity
- Options: create the right but not the obligation to buy or sell a quantity of an item at a set price on or before an expiration date

Key risks:

- Withdrawing assets by transferring the proceeds to unrelated accounts or high-risk countries
- Custodial relationships that allow the client to remain anonymous
- Movement of funds to disguise the origin
- Investing illegal proceeds

Trust & Company Service Providers

These create and administer companies. They:

- Form legal entities
- Act as directors, secretaries, partners
- Provide registered offices, business addresses
- Act as a trustee of an express trust
- Act as a nominee shareholder on behalf of another person
- Many of these activities can be performed by lawyers under legal privilege provisions which prevent the disclosure of information.

Real Estate Industry

- Investing illicit funds into real estate is common, because houses provide shelter for criminals; rural properties can be used for growing and storing drugs. The proceeds of crime can be used to pay deposits/down payments, mortgages, and construction costs. Using nominees to hide the beneficial owner is common.
- Buying and selling real estate is used in layering or integration for example, where a holiday resort can be purchased.
- Escrow accounts are used to hold funds for the purchase, and these accounts have many deposits and withdrawals related to the sale. They can be used to disguise criminal transactions that look like legitimate business transactions related to the sale or purchase of a property. As a result escrow accounts require specific monitoring.

Reverse Flip

A technique where an asset is apparently acquired for less than the normal price. This is paid for partly in clean money and partly in dirty money. For example, a $2M house could be acquired for $1M plus a further $1M of dirty money outside of the transaction ('under the table'). The property is later sold for the full $2M which is now all clean money.

Loan back

Dirty money is placed in the account of an offshore entity that is owned by the criminal. The offshore location means that the beneficial owner is difficult or impossible to determine. The offshore entity then makes a loan to the criminal which is clean money. In addition, repayments on the loan are also tax-deductible.

Manipulation of import/export prices

A technique where goods are shipped and the buyer either under- or over-pays. This allows monetary worth to move from one country to

another. It may also be used to avoid taxes. They are known as fraudulent transfer pricing schemes. Often exports are under-valued, because governments scrutinise imports so that they collect import taxes.

Letters of Credit

Letters of credit (L/Cs) are normally used to ensure that an exporter is paid for the goods they are exporting. The buyer of the goods will purchase a letter of credit from their bank, and forward it to exporter, who lodges it at their bank. Payments will be released by the buyer's bank when the conditions of the L/C are fulfilled – these are sometimes stage payments such as when goods are loaded onto a shipping carrier, when they arrive in the country, and when they are cleared by customs.

L/Cs facilitate money laundering by allowing funds to move country when they don't relate to an actual shipment, which is achieved in countries with lax export controls. L/Cs can be used when import and export prices are manipulated for money laundering or tax evasion purposes.

Black Market Peso Exchange (BMPE)

Money in the US or other drug consuming countries is purchased by agents working on behalf of drug producing countries. They deposit the cash into accounts they control, and use these funds to purchase goods in the drug consuming country. These goods are then shipped to the drug producing country and sold, with the proceeds handed to the drug producers.

Online/Internet Banking

- Helps create distance between customer and the bank, by eliminating face to face contact
- Cross border transactions from anywhere on earth
- Rapid execution of instructions
- To counter the threat, log files should be kept, including the IP addresses of access, maintained for at least a year.

Internet Casinos

- Transactions are primarily using debit or credit cards, and the casinos are located in unregulated off-shore locations so prosecuting individuals is difficult. Credit card transactions are identified by codes which enable such transactions to be blocked by banks and credit card companies.
- Online gambling is not used for cash movement as there is no physical presence to pay in cash.

Prepaid Cards and E-cash

- Prepaid cards are gift cards or Visa and MasterCard branded payment cards, portable, valuable, exchangeable for cash or products (via an ATM or shop purchase), and anonymous. Key risks:
- Anonymous card holders and funding, access to funds
- High value limits, and no limits to the number of cards that can be acquired
- Global access to cash at ATMs
- Offshore card issuers
- Substitute for bulk-cash smuggling
- There are some regulatory discrepancies over prepaid cards – in Germany adding value is considered the same as making a deposit, so prepaid card institutions are considered credit institutions, and are regulated. In the US regulations do not exist that cover such situations.
- Stored value cards (or electronic purses) hold the funds physically on a chip inside a card.

Ways to reduce risk:

- Limit the functions and capacity of smart cards
- Link new payment technologies to financial institutions and bank accounts
- Require standard documentation and recordkeeping
- Allow the examination of records by investigating authorities

- Establish international standards for the above measures

Name	Description	Anonymity	Reloadable	Value stored on card	Examples
Open system cards	A Visa, MasterCard, or American Express card that can be used in ATMs and retailers	Usually not, often embossed with the card-holders name	Yes: electronic banking, via retailers	Usually no – transactions authorised in real-time	Visa or MasterCard prepaid cards
Semi-open system cards	Same as open cards, without ATM access (purchase only)	No – same as open cards	Yes	Usually yes – lost and stolen cards/vouchers cannot be replaced	
Closed system cards	For buying goods from participating retailer.	Typically yes	Often not, but some cards can be reloaded	Usually yes – lost and stolen cards/vouchers cannot be replaced	Proprietary gift cards
Semi-closed system cards	Can be used at selected retailers	Usually yes	Often not, sold at pre-set denominations	Usually yes – lost and stolen cards/vouchers cannot be replaced	Gift cards or vouchers that can be used at a range of merchants.

Structures Designed to Hide Beneficial Ownership

Shell Companies

- Shelf company: A corporation without any activity, waiting to be sold as a ready-made company
- Shell company: A corporation which at the time of incorporation has no significant assets or operations

They can be used for legitimate purposes (tax and estate planning, mergers and acquisitions) and also by money launderers. They can issue shares to natural or legal persons, and in registered or bearer form. Bearer shares mean that whoever physically holds the share certificate, owns the share. They can be created for a single purpose or to hold a single asset.

Shell companies convert cash proceeds of crime into alternative assets. The launderer can create the illusion of business activity by creating a fictitious but cash-rich business (restaurant etc.). Any criminally controlled company can offer the criminal employment in order to appear legitimate.

Shell companies can disguise ownership. Nominees can be used as owners, directors, shareholders. Criminals can avoid being linked to assets by registering these assets in the name of a company. The records can be held in offshore locations where the information is difficult to access by law enforcement. In many cases the beneficial ownership information, if collected, is not verified in any way.

Front Companies

Launderers can also use legitimate businesses that offer a service, and comingle illicit funds with legitimate proceeds from the business. Such criminally controlled companies often use nominee owners or directors to hide beneficial ownership.

Selling these criminal companies is a way to create legitimate funds for the launderer, and they often get high prices as the turnover appears artificially high.

Buying a company already owned by the criminal

This is a way of repatriating funds. The criminal business is bought by an offshore company that was used to hide the criminal's funds. In this way the funds are repatriated, and appear as the legitimate proceeds of the sale.

Double invoicing

An offshore company orders goods from an onshore subsidiary. The payment is sent in full to their account. The payment is actually repatriating funds that have been spirited out of the country. If the subsidiary was over charged, they will show lower profits, reducing tax. This can also work in reverse where the subsidiary purchases from the parent at too high a price.

Trusts

These differ by jurisdiction, but generally the legal relationship is set up by a settlor, where assets are put into the trust for the benefit of one or more beneficiaries (or for a stated purpose, such as a charitable trust).

Trust accounts are very useful for money laundering, hiding beneficial owners, converting between assets, and processing illicit funds. They can also be formed in privacy havens making details about them impossible to locate.

Payments to beneficiaries can also be used as they don't require any justification as to the source of the wealth.

Bearer Bonds, Securities & Cheques

Bearer bonds and shares have no registry of owners, so physical possession is ownership. Banks should ask questions about the beneficial owners of such entities and share this information with law enforcement.

A bearer cheque is a cheque that can be paid out to the holder, usually without any identification. A non-bearer cheque can be converted into bearer form if the original payee has endorsed it.

Terrorist Financing

Money laundering is always about money received for illegal activity. Terrorist financing however may use legitimate funds for illegal activities.

Terrorists wish to disguise the link between their funding source and themselves so many of the layering techniques are used.

Key suspicious items:

- Account holders name on a list of suspected terrorists
- Frequent large cash deposits in a non-profit's account
- High volume of transactions
- Lack of clear relationship between activity and account holders business
- Large cash deposits followed by frequent withdrawals until the funds are depleted

Informal Value Transfer Systems

- Alternative money remittance systems: Hawala, poey kuan, Chop shop, hundi. It is cheaper than sending international transfers.
- Similar to Western Union® in operation:
    - A customer attends a local business such as a trading business and deposits funds, asking that they be sent to another country. The customer receives a code which they communicate to their beneficiary, which enables them to collect the funds
    - The trader then asks his counterparty in another country to make the funds available upon production of the code.
    - The debt between the two traders is either settled as part of the usual trade process, or is balanced by incoming remittances
- It can be used in any phase of money laundering
- There is very little paper trail maintained

Charities & Non-for-profits

- Charities are cash intensive, have considerable funds, often with a global presence, minimal oversight or regulation.
- To minimise risks, charities should have full budgets and account for all expenses, conduct independent audits and perform field audits to ensure funds are being used for legitimate purposes.
- Standard bank accounts should be used to ensure the normal banking system controls are in place.

Chapter 3 – Regulatory Framework

Compliance Standards for AML and Combating Financing of Terrorism

FATF was launched in 1989 by the G7, and is based at the OECD (Organization for Economic Cooperation and Development) in Paris.

There are 38 members, comprised of 36 jurisdictions, and 2 regions (GCC, Gulf Cooperation Council, and EU). There are 29 regional and international organizations that are associate members or observers, and participate in the work of the FATF.

Members:

Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Greece, Hong Kong (China), Iceland, India, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Portugal, the Russian Federation, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

Although the GCC is a member, the individual member countries of the GCC are not members, this is Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

To be a member, the jurisdiction must be strategically important (by GDP, size of banking sector, or impact to the global financial system), and lead to a more balanced geographic spread of members.

It also should provide political commitment to the 40 recommendations, and AML/CFT, agree to implement all 40 recommendations within 3 years, be assessed for compliance periodically, and actively participate in FATF. The country should also be a member of the regional FATF member.

The compliance criteria must be met in relation to:

- Money laundering and terrorist financing offenses
- Freezing and confiscation
- Customer due diligence (although there is some flexibility in this requirement)
- Record-keeping
- Suspicious transaction reporting
- Financial sector supervision
- International cooperation

Objectives of FATF:

- Promote AML messages worldwide
- Monitor implementation of recommendations by members (annual self-assessment, plus periodic visit from another member)
- Monitoring money laundering trends/countermeasures (the 'typologies' exercise)

- FATF cannot impose fines or other penalties, if members do not comply it applies a graduated approach of enhanced peer pressure, including putting the jurisdiction on a watch list, and ultimately rejecting the member.

40 Recommendations

- First issued in 1990, revised in 1996, 2003 and 2012.
- Interpretive notes clarify the application of specific recommendations
- After September 11 2001 terrorist attacks, they issued 9 recommendations on terrorist financing: 8 were adopted on Oct 31, 2001, and one was Oct 22, 2004.

- The 2012 version of the 40 recommendations combined the 9 into the 40.

Recommendations cover:

- Identify risk and develop policies
- Criminal justice system and law enforcement
- Financial system and regulation
- Transparency of legal persons and arrangements
- International cooperation

- 2003 revisions expanded the global reach of ways to crack down on the illicit movement of funds, it also strengthened measures to combat money laundering and terrorist financing.

Key changes in 2003:

- Included terrorist financing
- Included real estate agents, precious metals dealers, accountants, lawyers, trust services providers
- Specified procedures on customer identification, due diligence, including extra ID for high risk customers
- Clear definition of predicate offenses for money laundering
- Prohibited shell banks, urged transparency over legal persons
- International cooperation in terrorist financing investigations

2012 revision introduced:

- The risk assessment as the first step
- Incorporated the 9 terrorist financing recommendations into the main 40
- Measures against weapons of mass destruction
- Domestic PEPs and those with prominent functions in international organizations
- Identifying risks of new products prior to launch
- Financial groups should have a group-wide AML/CFT program
- Include tax crimes within the scope of predicate offenses

Overview of the 40 recommendations

Group	Topic	Recommendations
I	• AML/CFT Policies & Coordination • Assessing risks and applying a risk based approach • National cooperation and coordination	1-2
II	• Money laundering and confiscation • Money laundering offence • Confiscation and provisional measures	3-4
III	• Terrorist financing and financing of proliferation • Terrorist financing offence • Targeted financial sanctions related to proliferation • Non-profit organizations	5-8

Group	Topic	Recommendations
IV	• Financial and non-financial institution measures • Financial institution secrecy laws • Customer due diligence and record keeping • Additional measures for specific customers and activities • Reliance, controls and financial groups • Reporting of suspicious transactions • Designated non-financial businesses and professions	9-23
V	• Transparency and beneficial ownership of legal persons and arrangements • Transparency and beneficial ownership of legal persons • Transparency and beneficial ownership of legal arrangements	24-25

Group	Topic	Recommendations
VI	• Powers and responsibilities of competent authorities and other institutional measures • Regulation and supervision • Operational and law enforcement • General requirements • Sanctions	26-35
VII	• International cooperation • International instruments • Mutual legal assistance • Mutual legal assistance: freezing and confiscation • Extradition • Other forms of international cooperation	36-40

Key highlights of the 40 recommendations

- Risk based approach: countries and financial institutions should understand the risks they face, and take measures against those risks. This allows limited resources to be targeted.
- Designated categories of offenses: where the money derived from the specific offense is concealed in the financial system, this would constitute criminal money laundering. Countries should also confiscate the proceeds of crime.
- Terrorist financing and proliferation: countries should criminalize terrorist financing, freeze the assets of any entity that is identified by the UN Security Council as involved in terrorism. Also control against the use of non-profits for terrorist support.
- Knowledge and criminal liability: willful blindness (deliberate avoidance of knowledge of the facts) should not shield an entity from money laundering offences. Civil, or if possible, criminal offenses should apply to legal entities.
- Customer due diligence: should occur when business relations are started, when occasional transactions occur above a specified threshold, suspicions of money laundering or terrorist financing arise, doubts about previous customer identification exist.

Financial institutions should:

- Identify customers on a risk basis and verify their identity using independent source documents.
- Identify the beneficial owner and verify their identity.
- Understand the nature of the business relationship.
- Scrutinize transactions and ensure they match the knowledge of the customer.
- Maintain records.

Heightened CDD is recommended on the following:

- PEPs including verifying source of funds.
- Cross-Border correspondent banking, understanding the respondent's business and customers, levels of AML controls, mitigate risks of payable through accounts.
- Money or value transfer services (MVTS) should be licensed and be subject to AML requirements.
- New technologies should be risk-assessed, especially new products, delivery mechanisms and business practices. Risks should be mitigated.
- Wire transfers – accurate originator, intermediary and beneficiary information, and monitor for missing data, also sanctions screen the data.
- Suspicious transaction reporting: institutions must report to the FIU any suspicions.
- Expanded coverage of industries:
    - Casinos
    - Real estate agents
    - Dealers in precious metals and stones
    - Lawyers
    - Notaries
    - Accountants
    - Legal professionals (when they manage client money or other assets, buy or sell real estate, create or manage companies)
    - Trust and company service providers (when they act as formation agents, act as a director or secretary, act as a trustee or nominee shareholder for another person)

FATF designated thresholds:

- Financial institutions for occasional customers: €15,000.
- Casinos, including internet: €3,000.
- Dealers in precious metals and stones, when dealing in cash €15,000.
- Transparency and beneficial ownership of legal persons: particularly those that issue bearer shares.

- Powers and responsibilities of authorities: ensure FATF recommendations are being implemented in financial institutions, and are not owned or controlled by criminals.
- International co-operation and mutual assistance.

Non-Cooperative Counties

FATF identifies non-cooperative countries assessing them on 4 criteria:

- Loopholes in financial regulations: including inadequate supervision or creation of financial institutions, excessive secrecy, and lack of suspicious transaction reporting.
- Obstacles raised by regulatory requirements: inadequate business registrations, lack of beneficial owner information.
- Obstacles to international cooperation: administrative or judicial blockages.
- Inadequate resources for AML efforts, including the absence of an FIU
- Nigeria and Myanmar were the last two countries to be removed from the list in 2006.
- FATF now risk rates jurisdictions based on the compliance with the above.

Basel Committee on Banking Supervision

- Established in 1974 by central bank governors of the G10. The Secretariat is provided by the Bank for International Settlements (BIS) in Switzerland, which promotes financial stability among central banks and international organizations. Central bankers are not directly responsible for AML, but they can enforce high ethical standards.
- The Basel Committee's members are Argentina, Australia, Belgium, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Luxembourg, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

- In 1998, Basel Committee set out a statement of principles entitled "Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering" covering:
    - Customer identification
    - Compliance with laws
    - Conformity with high ethical standards and local laws and regulations
    - Full cooperation with national law enforcement to the extent permitted without breaching customer confidentiality
    - Staff training
    - Record keeping and audits
- They stressed confidentiality, as this was a time before legislation that required the identification of customers.

- In 1997 the Basel committee issued the "Core Principles for Effective Banking Supervision" that required strong KYC, and high ethical standards to prevent the use of the financial system by criminals. It also urged adoption of the FATF 40 recommendations.

- In October 2001 paper "Customer Due Diligence for Banks" covered:
    - Introduction
    - Importance of KYC standards for supervisors and banks
    - Essential elements of KYC standards
    - The role of supervisors
    - Implementation of KYC standards in a cross-border context

- The paper indicates that banks should monitor account activity and ensure that it is in line with expected usage. Numbered accounts are not prohibited, but the real customer's identification can't be hidden from compliance staff or regulators.

- The paper introduces 7 specific customer situations:
    - Trust, nominee and fiduciary accounts
    - Corporate vehicles, esp. with nominee shareholders or shares in bearer form
    - Introduced businesses
    - Client accounts opened by professional intermediaries (i.e. pooled accounts for mutual funds, pension funds, and money funds)
    - PEPs
    - Non-face to face customers
    - Correspondent banking

- The following recommendations are made:
    - Private banking should not be exempt from KYC
    - Customer acceptance should include the country, business and other risk factors and should indicate who is, and is not, an acceptable customer
    - Understand the beneficial owner
    - Periodic training on KYC & AML
    - Internal audit and compliance should regularly monitor staff performance and adherence to KYC policies
    - High risk accounts should be monitored for suspicious activities away from normal patterns of usage
    - Regulators should ensure staff follow KYC procedures

- The 4 key elements of KYC according to the paper are:
    - Customer identification
    - Risk management
    - Customer acceptance
    - Monitoring

EU Directives on Money Laundering

First Directive

Issued in 1991 as 91/308/EEC, requires member states to prevent domestic financial services being used for money laundering, amending national law if needed. It only covered drug trafficking (as defined by the 1988 Vienna Convention), however member states could broaden the predicate crimes.

Second Directive

Issued in 2001 as 2001/97/EEC; required stricter money laundering controls.

- It included all serious crimes as predicate crimes, including fraud
- It brought bureau de change and money remitters into scope
- It introduced 'willful blindness'
- A precise definition of laundering (i.e. concealing the criminal source of funds, or using property knowing it was from a criminal source)
- It went much further than US law, and even the FATF guidance
- It included lawyers moving money for clients, auditors, accountants, tax advisers, real estate agents, notaries, legal professionals

Third Directive

2005/60/EU is based on the FATF 40 recommendations, and was adopted in 2005, to be implemented by 2007.

- Defined money laundering and terrorist financing as separate crimes, and ensured that the directives covered both
- Risk based CDD – enhanced CDD for riskier customers
- Protect employees who report suspicious
- Collect stats on the SARs, e.g. number filed, follow-up performed, number of cases, prosecutions and convictions

- Financial institutions must record beneficial owner of accounts held by legal persons i.e. natural persons controlling 25% or more of a legal entity or person
- Defined PEPs as those in prominent positions and their publically known associates, ceasing to be a PEP after one year of not holding office

It applies to:

- Credit institutions
- Financial institutions
- Auditors, external accounts, tax advisors
- Legal professionals
- Estate agents

New for the third directive are:

- Trusts and company service providers
- Dealers selling goods for cash (>€15,000)
- Life insurance intermediaries

Regional FATF-Style Bodies and FATF Associate Members

There are eight regional FATF-style bodies and FATF Associate Members that have similar form and functions to those of FATF. Many FATF member countries are also members of these bodies.

Asia/Pacific Group on Money Laundering (APG)

- A Financial Action Task Force (FATF)-style autonomous voluntary and cooperative regional body, not derived from an international treaty, and not part of an international organization. Established in 1997 consisting of jurisdictions in the Asia/Pacific Region. See www.apgml.org

Caribbean Financial Action Task Force (CFATF)

- A FATF-style regional body comprising Caribbean states, including Aruba, the Bahamas, the British Virgin Islands, the Cayman Islands and Jamaica. Established as the result of meetings in 1990 and 1992. Cooperating nations include Canada, France, Mexico, the Netherlands, Spain, UK, US. 19 recommendations, revised in 1999 which complement the FATF 40. See www.cfatf.org

Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV)

- Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures. Formerly PC-R-EV, the committee was established in 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessments of anti-money laundering measures in place in Council of Europe countries that are not FATF members. MONEYVAL is a sub-committee of the European Committee on Crime Problems of the Council of Europe (CDPC).

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

- A FATF-style regional body comprising fourteen countries from the Eastern region of Africa down to the Southern tip of Africa. It was established in 1999. Has adopted the FATF 40 recommendations. See www.esaamlg.org

Eurasian Group (EAG)

- A FATF-style regional body formed in October 2004 in Moscow. Member countries include Belarus, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan. Observers include UK, USA, Italy, Georgia plus organizations such as FATF, World Bank, IMF. See http://www.eurasiangroup.org/

Financial Action Task Force of South America against Money Laundering (GAFISUD – Grupo de Acción Financiera de Sudamérica)

- A FATF-style regional body for South America, established in 2000. Members include: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Panama, Paraguay, Peru, and Uruguay. Created by inter-governmental treaty which permits more countries to join. Adopted the FATF recommendations. See http://www.gafisud.info/home.htm

Intergovernmental Action Group against Money-Laundering in West Africa (GIABA – Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Quest)

- No definition available

Middle East and North Africa Financial Action Task Force (MENAFATF)

- A FATF-style body established for the Middle Eastern and North African regions in 2004. Algeria, Lebanon, Saudi Arabia, Bahrain, Libya, Sudan, Egypt, Mauritania, Syria, Iraq, Morocco, Tunisia, Jordan, Oman, UAE, Kuwait, Qatar, Yemen. Voluntary, not derived from international treaty, independent from any other international organization. See www.menafatf.org

Other AML initiatives

CICAD (Organization of American States: Inter-American Drug Abuse Control Commission.

- 1992, OAS (Organization of American States) is a permanent international body which provided model legislation tackling money laundering. Forms Western Hemisphere's drug policy.
- 1999 a specialist AML unit (CICAD-AMLU) formed, which provides technical assistance and develops regulations (influenced by and compatible with FATF 40).
- They provide support to bankers and regulators, judges and prosecutors, financial intelligence units, law enforcement.

Egmont Group of Financial Intelligence Units

- 1995 FIUs worked together informally to reciprocate information, supply training, create the Egmont Secure Web (ESW) technology platform, promote operational autonomy, promote the establishment of further FIUs.
- It defined an FIU as: central, national agency for receiving analyzing and disseminating SARs related to money laundering and terrorist financing, as required by national legislation.
- In 2010 there were 117 Egmont members

Wolfsburg Group of Global Banks

- Association of 11 global banks, settings standards for KYC, AML, and terrorist financing policies.
- Created in 2000, principles carry no force of law or penalties.
- In partnership with Transparency International.
- Covers private banking.
- Indicates the following as high risk: PEPs, high risk countries (those without good AML standards), high risk activities (clients whose wealth originates from activities susceptible to money laundering).

- 2002, prohibited concentration accounts (internal non-client accounts) that sever the link between the source of funds.
- 2002, agreed how to deal with terrorist financing, by sharing lists of suspected terrorists globally, providing information on the methods used by terrorists, defining business guidelines for sectors and activities prone to terrorist financing, and develop uniform policies.
- Enhanced CDD for remittance services, exchange houses, bureau de change, money transfer agents, and underground banking businesses and alternative remittance systems.
- Correspondent banking services should not be provided to a shell bank, CDD should not be performed on IMF and World Bank.

Other International Organizations

- Any country wanting financial assistance from the World Bank and International Monetary Fund must have adequate AML controls.
- Other organizations with AML or anti-terrorist financing initiatives include:
    - African Development Bank
    - Asia Development Bank
    - The Commonwealth Secretariat
    - European Bank for Reconstruction and Development (EBRD)
    - European Central Bank (ECB)
    - Europol
    - Inter-American Development Bank (IADB)
    - Interpol
    - International Organization of Securities Commissions (IOSCO)
    - Offshore Group of Banking Supervisors (OGBS)
    - World Customs Organization (WCO)

Key US Legislation and Regulation relevant to International Transactions

USA Patriot Act

October 2001 strengthened money laundering laws introduced in 1986, and the Bank Secrecy Act in 1970.

Title III (public law 107-56) "International Money Laundering Abatement and Anti-terrorist Financing Act" of 2001 contains most of the AML content. It governs US and non-US financial institutions that operate in the US. It enables international access points to the US financial system to be controlled.

Section 311: special measures for primary money laundering concerns. Allows the US Treasury to specify as a specific money laundering concern: a foreign jurisdiction, a foreign financial institution, any type of international transaction, or a type of account. US banks would then need to take special measures with these types of concerns.

There are five, graduated special measures that can be taken:

1) Keep records, or file reports containing transaction data including beneficial owners as well as originator and beneficiary.

2) Keep information about the beneficial owner of any US account opened or maintained by a foreign person or their representative.

3) Identify and obtain information about customers who are permitted to use foreign bank's payable through accounts.

4) Identify and obtain information about customers who are permitted to use foreign bank's correspondent accounts.

5) Close certain PTA or correspondent accounts.

Section 312: Correspondent and Private banking

- Required due diligence or enhanced due diligence for foreign correspondent and private banking accounts for non-US persons. It covers almost all account relationships that can be held with a foreign financial institution.
- The rules apply to US banks, credit institutions, thrift institutions, trust banks, broker-dealers, futures commission merchants, and introducing brokers in commodities and mutual funds, and US-based agencies and branches of foreign banks.
- Foreign institutions includes: foreign banks, foreign branches of US banks, credit unions, foreign businesses that would be considered broker-dealers, futures commission merchants, introducing brokers in commodities or mutual funds if operated in the US, and foreign money transmitters or currency exchangers.

Due diligence should:

- Determine whether enhanced DD is needed
- Assess the money laundering risk associated with the correspondent account
- Use risk-based procedures and controls designed to detect and report suspected money laundering
- Enhanced DD should apply to a correspondent account for a foreign bank operating under:
- Off-shore banking license
- A license issued by an non-cooperative country
- A license issued by a country deemed a risk under section 311 of the Patriot Act.
- Private banking is deemed as an account with a minimum deposit of $1 million, assigned to a designed banker, for a non-US person
- All beneficial owners should be identified
- Verify whether an owner is a current or former senior foreign political figure

- Understand the purpose and use of the account, and the source of the funds
- Monitor the account to ensure the use is in line with expectations, reporting any suspicions

- Section 313 of the Act prohibited correspondent accounts for shell banks.

- Section 319(a) allows forfeit of funds from a US correspondent account of the same amount as those deposited in a foreign correspondent account.

- Section 319(b) records relating to correspondent accounts at foreign banks should be available within 120 hours (5 days).

OFAC: Office of Foreign Assets Control

- OFAC enforces foreign policy and national security goals by imposing economic and trade sanctions. They prohibit transactions and require blocking of assets that belong to people on their lists. They can apply significant sanctions for violations. The rules apply to all US citizens, no matter where they are located, all people in the United States, all US-incorporated entities and their foreign branches.

Key Groups

Group	Description	Key Documents
Financial Action Task Force on Money Laundering	• Intergovernmental body with 34 member countries and two international organizations. • Sets money laundering and terrorist financing standards.	• 40 Recommendations on Money Laundering and Terrorist Financing (Last updated February 2012).
Basel Committee on Banking Supervision	• Established by the central bank governors of the G-10. • Promotes sound supervisory standards worldwide.	• Customer Due Diligence for Banks Paper (2001). • Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (2002). • General Guide to Account Opening and Customer Identification (2003). • Consolidated KYC Risk Management Paper (2004).

Group	Description	Key Documents
European Union	• The EU Directives on anti-money laundering require the EU member states to issue legislation to prevent their domestic financial systems being used for money laundering.	• 1st EU Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (1991). • 2nd Directive (2001). • 3rd Directive (2005).
Wolfsburg Group	• Association of 11 global banks. • Aims to develop standards on money laundering controls for banks.	• Wolfsburg Anti-Money Laundering Principles for Private Banking (last updated 2002). • The Suppression of the Financing of Terrorism Guidelines (2002). • Anti-Money Laundering Principles for Correspondent Banking (2002).

Group	Description	Key Documents
APG, GAFISUD, CFATF, MENAFATF, Eurasian Group, Eastern and South African • *AML Group*	• FAFT-style regional bodies	• Typologies exercises (methods of money laundering)
Egmont Group	• Informal networking group for Financial Intelligence Units	• Statement of Purpose (last updated 2004). • Principles for Information Exchange between Financial Intelligence Units for Money Laundering Cases (2001). • Best Practices for the Exchange of Information Between Financial Intelligence Units (2004).
CICAD	Commission within the Organization of American States that deals with drug-related issues, including money laundering.	• Model Regulations

Group	Description	Key Documents
World Bank and International Monetary Fund	These organizations work together and in conjunction with FATF in encouraging countries to have adequate anti money laundering laws and reviewing the laws and procedures of FATF member countries.	Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: A Manual for Countries to Establish and Improve Their Institutional Framework 2002 (revised 2007).

Chronological AML Developments

Year	Developments
1986	• U.S. enacts its Money Laundering Control Act, codified at 18 U.S.C. Section 1956 and 1957, the first law in the world to make money laundering a crime.
1988	• Vienna Convention (UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances) is agreed. • Statement of principles is issued by Basel Committee on Banking Regulations and Supervisory Practices.
1989	• Financial Action Task Force established at G-7 economic summit in Paris.
1990	• FATF issues its 40 Recommendations on Money Laundering. • Caribbean Financial Action Task Force is established and issues CFATF 19 Recommendations on Money Laundering. • Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime is issued.
1991	• FATF members agree on "mutual assessment" process. • Council of Europe Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (91/308/EEC) is issued.
1992	• Organization of American States (OAS) model anti-money laundering regulations and legislation are adopted.

	• Kingston (Jamaica) Declaration on Money Laundering of the CFATF is issued.
1993	• UN model law on Money Laundering, Confiscation and International Cooperation in Relation to Drugs is proposed.
1995	• Egmont Group of Financial Intelligence Units is formed.
1996	• The FATF 40 Recommendations are revised to extend predicate offenses beyond drugs to other serious crimes. • The first FATF Typologies Report is released.
1997	• Asia/Pacific Group on Money Laundering (APG) is established. • PC-R-EV (now MONEYVAL) is established, which conducts self-assessments of AML measures in European countries that are not FATF members.
1998	• OAS Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses are amended.

Chapter 4 – AML Compliance

Anti-Money Laundering Compliance Program

Covers:

- What to consider when setting up an AML compliance program
- Assessing risk
- Identifying, managing, documenting and following-up any suspicions
- Knowing your customer and employee
- Auditing your program
- Training and screening employees

- Main aim is to protect the organisation from money laundering & terrorist financing, plus ensure compliance with all relevant laws and regulations by setting standards and policies for the organisation.
- It should be risk based – not all products and services, geographic regions, and customer types, and thus not all areas of the business pose the same risk of money laundering. Greater risks require greater controls. New products and services should be evaluated for risk and any necessary controls implemented prior to launch.
- The AML function can be stand-alone, or combined with other compliance duties, but must have a centralised aspect to ensure consistency. It should also address corporate governance and overall oversight.

Assessing Risk and Developing a Risk Scoring Model

Identify legal requirements, and supplement with FATF risk-based controls. Controls should be strong enough to counter the risk – low risks can be managed with minimal controls, high risk areas need robust controls. Controls include: verifying the identity of customers (KYC), customer due diligence (CDD), suspicious activity monitoring and economic sanctions screening.

Risk based approaches are more:

- Flexible: useful because risks vary across geographical areas, customers, products and delivery mechanisms, and over time.
- Effective: because companies know better than regulators how to mitigate money laundering risk.
- Proportionate: because risk based approaches allow a common sense and intelligent rather than check-box approach.

Levels of risk

- **Prohibited**: where the risk is so high, no dealings of this type will be performed by the company. Examples include shell bank customers, or sanctioned geographic regions e.g. Sudan or Iran.
- **High Risk**: significant risk exists, so enhanced controls are required e.g. enhanced monitoring and customer due diligence. Countries noted for drug trafficking, or corruption for example might be high risks, as might customers who are PEPs, and products such as correspondent and private banking.
- **Medium Risk**: more than just a standard risk of money laundering, and so merits additional controls.
- **Low (or Standard) Risk**: normal business rules apply, often domestic customers and FATF member countries are considered low risk.

- The risk of the geography, customer type, and products/services are each assigned a risk score e.g. 1-10 with 10 being high risk. These could then be aggregated, or weighted then aggregated. Certain combinations could also be assigned a higher significance if that leads to a higher perception of risk. The risk ranking should be re-evaluated periodically.

- Note that any 'prohibited' items would cause the relationship to be rejected.

- High risk relationships should warrant more attention, so the organisation should be careful to ensure that there is sufficient oversight if there are a lot of high risk customers as a proportion.

Geographical Location

- Both the residence and the citizenship of customers are important. Corporate headquarters and locations they carry out their business are also key. Check if any pose and increased risk of money laundering.

- Organisations need to develop and document a methodology for assessing geographical risk, including whether the county has FATF-style membership, high levels of corruption (Transparency International publish these each year), drug production or transit history, or is in a secrecy haven.

Customer Type

- There are various classes of clients, such as individuals, and different types of companies such as listed, private, partnerships, joint ventures, as well as various types of financial institutions.

- A history of involvement in criminal activity would warrant the highest level of risk. Political figures and those in political organisations are high as they may have access to corrupt funds. Directors of multinationals may be lower risk than directors of private companies due to the level of due diligence that is possible for a listed company.

- Company structures that offer some level of privacy (known as the 'Corporate Veil'), such as charities, limited companies, trusts, or other structures where it is difficult to identify the beneficial owners.

The following types of companies pose an increased level of money laundering risk:

- Casinos
- Companies and banks in tax and banking havens
- Leather goods stores
- Currency exchanges, money remitters, check cashers
- Car, boat and plane dealerships
- Used car and truck dealers, machine parts
- Travel agencies
- Brokers/dealers in securities
- Precious metal and stones dealers
- Import/export companies
- Cash-intensive businesses – restaurants, retail, parking, car wash
- Telemarketing – which is linked to 'Boiler Room' scams

Products and Services Risk

Review your products and services to determine how they might be used to launder money or finance terrorism. Key risk factors might include the ability to pay third parties, complexity or anonymity, or minimal oversight.

The following specific banking products are considered high-risk:

- Private banking
- Offshore international activity
- Deposit taking facilities
- Wire transfer and cash management functions
- Transactions where the beneficiary is hidden
- Loan guarantee schemes (where some or all of the loan is guaranteed by a third party)
- Travellers cheques, bank cheques, money orders
- Foreign exchange
- Trade financing with unusual pricing features
- Payable through accounts (PTAs)

The Elements of an AML Program

An organisation must address the following:

- Internal policies, procedures and controls
- Designated compliance officer with day to day oversight of the program
- On-going employee training
- Independent audit function to test the program

Internal policies, procedures and controls

- Polices are a high-level statement of principles. Procedures and controls translate this into the details of how to execute and validate success in implementation of those principles. Controls might include dual controls such as secondary review, or technology controls that prevent or detect certain incidents.

- Check what laws and regulations apply, this will set the minimum compliance level. Then based on the risk assessment, and risk appetite, you should prohibit anything the organisation deems too risky i.e. regions, company types or customer types. You also need to monitor laws and regulations for changes. The policies should be approved by upper management or the board of directors.

Key aspects of the policies, procedures and controls:

- Identify high risk products, services, customers and geographic regions
- Be tailored to organisation risk
- Inform the board and senior management of key initiatives, deficiencies, details of suspicious reports filed, and actions taken
- Clear accountability for all duties undertaken under the program
- Ensure continuity despite staff changes
- Meet all regulatory requirements and recommendations

- Annually review the program, and update timely in response to changes in regulations
- Include risk-based customer due diligence
- Include controls and monitoring systems to detect and report suspicions. The reporting should be centralised for consistency.
- Dual controls/segregation of duties: those who complete forms should not submit them or grant exceptions
- Comply with record keeping requirements
- Include supervision of employees engaged in any AML activity
- Train employees on their obligations
- Include AML in job descriptions
- Screen new employees, and provide sanctions for employees who fail in their AML duties
- Test the effectiveness of AML controls, policies and procedures, separate from internal audit

Designated compliance officer with day-to-day oversight of the program

Responsible for:

- Designing, implementing, and changing the AML program
- Communicating successes and failures to management
- Creating training
- Staying current with regulatory & legal changes

- Some departments are just one person, others are split into strategic and operational (i.e. monitoring and reporting) aspects.

Possible subgroups in the department could include:

- Investigations – which monitor automated alerts and referrals from other staff, files SARs
- Business Support – performs CDD on higher risk clients, acts as a point of contact for queries
- Oversight – reviews and updates the program and associated procedures, monitors the legal and regulatory environment.

Coordinates regulatory exams with the business. May also prepare training and provide guidance on complex AML issues.

- In addition, within the business, there are AML activities where there is customer contact e.g. CDD.

On-going employee training

- Can include formal training, as well as emails, newsletters and team meetings with AML content. Most areas of the business should have AML training, and it should include most staff. The training should only cover items relevant for those staff, and include real life examples. Attendance or performance should be tracked, with failure to attend or achieve a minimum score addressed through disciplinary procedures.

Key training by staff type:

- Customer-facing: this is the front line of defence; they need a deep practical understanding of AML. Cash handing staff need to know how to identify suspicious cash transactions, credit officers need an understanding of how credit can be used for AML purposes.
- Back office: cash vault, wire transfers, trade finance all need specialist training. Many back office roles may only require general training.
- Audit and compliance: training on changes in regulation and law, money laundering methods and enforcement.
- AML Compliance: training to stay on top of changes e.g. attending conferences.
- Senior managers & board of directors: strong board support is needed and AML should be regularly communicated, they need understanding in line with their responsibility.

Training topics:

- General information/background, importance of AML

- Legal framework & applicability to organisation and staff
- Penalties – disciplinary action, fines and jail
- How to deal with suspicions
- Internal policies & procedures

Independent audit function to test the program

- The audit must be carried out by people not involved in the AML program, who report directly to the board of directors or to a designated board committee comprised of more than half outside directors. Auditors should be qualified to perform the audit.

The audit should cover:

- Adequacy of risk assessment, CCD policies, procedures and processes
- Adherence to the above
- Testing of high risk transactions (i.e. high risk products/services/customers/locations)
- Adequacy of training
- Compliance with laws and regulations
- Integrity and accuracy of AML systems
- Assess suspicious activity monitoring by:
- Evaluating policies and procedures
- Reviewing the system's method for identifying suspicions
- Evaluating the reports produced
- Checking any filtering criteria
- Where systems are not used, a review of the manual transactions should check that large or suspicious transactions were appropriately dealt with
- Evaluate how suspicious transaction reports (STRs) are researched and evaluated

Compliance Culture

- Compliance should be everyone's role, supported by top management. The board should approve the AML program, and are responsible for implementing any examiners or internal audit recommendations.
- The AML officer has to ensure that management see the cost of the program as essential to mitigate reputational and financial risk.
- CDD information can be used to cross sell other products.
- Compliance staff should not have bonuses tied to the performance of business units.
- Compliance staff can be close to the business, but must report outside to ensure independence.

Customer Due Diligence

There are 7 elements to CDD:

- Identify the customer/beneficial owner & source of funds/wealth
- Profiles of expected activity
- Approval for specific products/services
- Assessment of the risks of the customer
- Monitoring of account & transactions
- Investigation of unusual activity
- Document findings

- CCD should be consolidated across all regions and all products sold to the customer by an institution.

Account opening guidelines from Basel 2003

- Legal name, and previous names
- Address
- Phone and email
- Date and place of birth
- Nationality
- Occupation, position, employer

- A unique identifier from a government issued document (passport, driver licence)
- Signature
- Verify this by checking the date of birth against a government ID, the address using an official letter, contacting the customer using phone, email and mail addresses. Check the official documentation by physically inspecting it, or checking with a government agency.
- The source of wealth and funds should be validated, and any deposits not in line with this should be investigated.
- The proximity of the customer to the branch should be checked and if not close by, check why.
- Equally effective CDD should apply to non-face-to-face customers.
- For businesses, obtain the name, mailing address, business location, contact people and phone/address details, official identification number (e.g. tax number), the certificate of incorporation, memorandum and articles of association, nature and purpose of the business.
- Verify this by reviewing the latest accounts; use a business information service or an undertaking from a lawyer or accountant.
- This should be codified in a Customer Identification Program (CIP).

Name lists

All customers should be checked against lists of known undesirables such as OFAC.

- There are difficulties identifying PEPs because although lists of such people are kept, the information is incomplete (i.e. no date of birth). This will likely cause issues with large retail bank, who may find many matches.

Arabic Names

- All names are translated (transliterated) from Arabic script.
- Short vowels are often left out/altered e.g. Mohammed could be Mohamad or Mohamed.

- Names are often long, with the second name being the father's name.
- If bin or ibn precedes the name, it means 'son of'.
- If a family name is appended, it sometimes includes 'al'.
- Common names are Mohammed, Ahmed, Ali and any name beginning Abd- or Abdul which means 'servant of ' which is then followed by one of 99 suffixes which describe God.
- Many names begin 'Abu' meaning father of, followed by a noun that may mean 'freedom' or 'struggle'. If this is a first name, it is not usually a given name. Only when Abu is a prefix of a surname should it be accepted as a correct name.

Know Your Employee

Insiders can pose the same threat as a customer. Perform background screening for criminal history. Contractors should be subject to the same controls. Consider re-screening as circumstances change e.g. promotion. The FDIC issued guidance on this in 2005.

Suspicious/Unusual Transaction Monitoring and Reporting

Any activity that is not consistent with a customer's source of income or regular business. The system should be risk based (as there are so many transactions to monitor, they can't all be monitored). Some items that can be monitored:

- Daily cash in excess of reporting threshold
- Daily cash just under reporting threshold
- Cash activity over time to detect structuring
- Wire transfer reports per country and value
- Monetary instrument activity
- Check kiting/drawing on uncollected funds
- Significant change reports (i.e. beneficial owners, addresses, new cards out to new addresses)
- Activity on new accounts

Typical reporting process is:

- Procedures to identify potential suspicious transactions
- Formal evaluation of the activity and any continuation
- Documentation of the decision
- Procedures to notify senior management/board of directors of SARs
- Training on detecting suspicious transactions

Red Flags

Customers

- International use of ATMs
- Customers who move frequently
- Opening deposits such as international wires, large cash sums
- Customers who are not local – ask why you won the business
- Credit balances – customers who over pay on credit line or card accounts
- Common addresses, IP addresses, phone numbers – unrelated customers who share data points could be suspicious. Customers who change their information after opening an account to a shared data point are particularly suspicious.
- Customer discusses record keeping requirements, or is nervous or threatening
- Customer will not proceed with a transaction once they are informed that it is reportable
- Customers who offer bribes
- Irrational behaviour, such as turning down a better interest rate

Cash transactions

- Large cash deposits without counting the cash
- Exchanging small bills for large bills
- Cash deposits contain fake bills, musty or very dirty bills
- Students who have access to large sums of money
- Offshore institutions whose names resemble well known institutions
- Transaction includes offshore islands or locations difficult to find on a map
- Customer performs FX without caring about spread
- Telephone number disconnected
- Customer does not want any mail
- Customer deposits cash wrapped in currency straps

Non-cash deposits

- Frequent purchase of monetary instruments
- Deposits travellers cheques in same denomination and serial number sequence or consecutively numbered monetary instruments
- Deposits third party cheques

Wires

- Incoming wire with instructions to convert to cashiers cheques and to mail them out
- Wire transfers to secrecy havens
- Customer moves 'profits' out of the country

Safe deposit activity

- Spending unusual amount of time in a safe deposit box area (indicating the keeping of large cash amounts)
- Renting multiple safe deposit boxes

Credit transactions

- A transaction is made to appear more complex than it needs to be by use of nonsensical terms such as emission rate, prime bank notes, standby commitment, arbitrage or hedge contracts
- Customer requests loans made to offshore companies or secured by obligations in offshore banks
- Customer suddenly pays off large problem loan, without any obvious source of funds
- Customer collateralises loan with cash or certificates of deposit

Commercial account activity

- Check cashing business that does not withdraw cash indicating it has another source of the cash
- Corporate account shows no periodic activity

Trade finance

- Import or export of items at prices above or below normal market rates
- Changes to letter of credit beneficiary just before payment is made
- Change to the place of payment to an account in another country to the beneficiaries stated location
- LOC is not in line with customer business
- LOC is for goods not in demand in the importing country
- LOC is for goods that are not produced in the exporting country
- Commodities are shipped through locations without an apparent economic or logistical reason

Investment accounts

- Uses investment account as a pass-through vehicle for offshore wires
- Customer not interested in usual decisions around fees or investment vehicles
- Deposits of cash, money orders, travellers cheques, or cashiers cheques under the reporting threshold in order to fund the account
- Customer cashes out investments such as annuities or life insurance early

Employees

- Employee exaggerates the resources of a customer
- Employee involved in excessive number of unresolved exceptions
- Leads lavish lifestyle not in line with salary
- Overrides internal controls or circumvents policy
- Avoids taking periodic vacations

Money remitter/ currency exchange house

- Unusual use of money orders, travellers checks or funds transfers
- Two or more people working together on transactions
- Transactions under the reporting threshold

Insurance companies

- Cash payments on insurance policies
- Refunds requested during cancellation period
- Policy payments made from abroad
- Beneficiary of policy has no relation to the policy owner
- Unconcerned with penalties for early redemption
- Bonds sold in one jurisdiction that are redeemed by an entity in another jurisdiction

Broker-Dealers

- The customer is acting as an agent for an undisclosed beneficiary
- Large number of accounts, with transactions between them, without just cause
- Unexplained wire activity
- Deposits made to fund an investment account that are then withdrawn
- Penny stock, Regulation S stock and bearer bonds activity, which have all been associated with money laundering

Black Market Peso Exchange Indicators

- Payments made in cash or by wire by a third party
- Use of third party cheques, bank drafts or money orders
- Structured currency deposits under the reporting threshold
- Consumer checking accounts that become dormant
- Personal checking accounts opened by foreign nationals who come into the bank together
- Multiple accounts opened the same day
- Increases in the amounts of currency deposits by US businesses that export to Columbia

Electronic AML Solutions

Examples:

- Transaction monitoring – scanning the transactions for laundering activity
- Watch list filtering – screening new accounts, existing customers, beneficiaries and counterparties against lists of known criminals and terrorists
- Automation of regulatory reporting – such as currency transaction report (CTRs) or suspicious transaction reports (STRs)
- Maintenance of audit trail

Chapter 5 - Investigations

Conducting and responding to an investigation

Law enforcement investigations

These are normally triggered by STRs, tip offs, or other cases. The requests arrive in the form of a subpoena or search warrant. Subpoenas are issued by grand juries and empower law enforcement to obtain evidence (i.e. documents & testimony).

A search warrant allows law enforcement to enter a specific location and seize specific categories of items of documents. It doesn't force testimony. In the US and other jurisdictions, banking regulators have the power to inspect all bank books and records as they see fit.

The 10 steps law enforcement takes are as follows:

- Follow the money: either where the money originated or ended up to understand the flow
- Identify the unlawful activity: i.e. what is the predicate offense (could be widely defined as: "any proceeds from criminal activity")
- Document activity and transactions: both the predicate offense and the flow of money
- Review databases: financial intelligence unit (FIU) database and commercial databases can provide very useful and extensive financial information, plus other governmental databases such as social security and tax records
- Review public information: court records, company filings, credit reports can contain useful background
- Review licensing and registration files: e.g. vehicle registration documents
- Analyse financial transactions: identify any unusual flows or amounts

- Review STRs for any linked activity
- Conduct computer-based searches
- Obtain international co-operation: for cross-border cases

Decision to prosecute the institution

This will be made based on whether the institution has a criminal history, has cooperated, whether the institution identified and self-reported, there was a comprehensive AML program in place, took timely remedial action, whether civil or criminal procedures would be best suited, whether a deterrent to others would warrant a prosecution.

Responding to a law enforcement investigation

Respond quickly and completely to all requests. If the request is overly broad or intrusive, you can seek to narrow the request. First ensure senior management is informed (include legal) and establish the point person to respond. If the enquiry is aimed at the institution, not a customer, the board of directors should be informed. Check all requests for any risk to the institution. Do not provide information to anyone who may be implicated in the proceedings.

The institution should conduct an enquiry of its own to establish the facts; determine the institution's exposure, and what steps may need to be taken.

Summonses and Subpoenas

Senior management and/or legal counsel should review. If there are no grounds for contesting, then take all possible measures to comply timely and completely. Do not notify the customer. If there is a requirement to keep the account open, this must be obtained in writing on letterhead, with the proper authority.

Search Warrants

These are not open-ended; agents can enter the premises, and look for and seize certain documents. A warrant does not compel a testimony.

Take the following steps:

- Call legal counsel
- Review the warrant to understand the scope
- Obtain a copy of the warrant
- Ask for the affidavit that accompanies the warrant (if you are allowed to see it, it will provide some context to the warrant)
- Watch the agents perform their search, make a record of any seized items
- Ask for the agents inventory of items seized
- Note the names and agency affiliations of the agents

- Documents and computer records that are protected by attorney-client privilege should be marked and retained in a separate area. If agents wish to seize these, suggest that they be given to the court for safe keeping.

Orders to restrain or freeze accounts or assets

- Only freeze once you have a copy of the warrant issued by a court requiring the freezing of the funds or account.

Dealing with Investigators and Prosecutors

- The most effective strategy is to cooperate. Provide them the information that they need, even if they don't have a warrant or subpoena. Make officers available for interview. It may also include releasing any management report into the matter. Maintain a good working relationship which will allow the organization to conduct a parallel investigation which will enable the institution to be prepared for enquiries.
- Try to learn how the prosecutors view the facts, and correct those that are inaccurate.

Obtaining Counsel for the Investigation

- If the investigation appears to have risks to the institution, counsel should be sought. Internal counsel will have a better understanding of the organization, however if the case appears to have criminal implications, outside counsel may be better. Ensure that in-house or external counsel is sufficiently experienced and knowledgeable with regard to the legal and factual issues involved.

Notices to Employees

- For government investigations, ensure that staff know that documents should be handed over to a central contact who can co-ordinate handing documents over to investigators. The institution can also determine what (if anything) can be contested.

Media Relations

- Public perception is vital to maintain trust of the institution and their officers. If the facts are against the institution it may be best to provide 'no comment' to the press, any false or misleading statements will make the matter worse in the long run. False

statements by a publically traded company could lead to an SEC review or law enforcement action.

Internal Investigations

Should be conducted when:

- A report of an examination is received from regulators
- Third party information is received
- Surveillance of monitoring systems indicate issues
- Employee hotline tip offs
- Government subpoenas or search warrants
- Government is asking questions about the institution, competitors, customers or business practices
- A civil lawsuit is filed against the institution

- Document the purpose, scope, method and conclusions of the investigation.

Closing the Account

Consider the following attributes:

- What is the legal basis for closure?
- The policies and procedures and terms and conditions around closure?
- How serious is the conduct? If it is serious and is of the level where you would normally close the account, then close the account.

Conducting the Investigation

- Review documents, interview employees and issue a report. Decide whether to involve counsel. Keep senior management, and if necessary the Board informed of the scope and progress.

Documents

- All documents should be kept in line with legal retention timescales – US 5 years. Information can be useful from statements, signatures, checks, loan documentation, correspondence etc. Ensure that important documents are not lost, altered or destroyed. You can send a memo informing staff of the retention requirement, however, if this might prompt someone to destroy or alter documents, deal with that separately.

- Ensure the document destruction policy does not destroy documents that should be retained for law enforcement.

- It is OK to destroy documents in line with the destruction policy prior to notification of a government investigation, but not after.

Interviewing Employees

- This should be done as soon as possible while memories are still fresh. Counsel should prepare staff prior to investigator interviews to understand the process, and also debrief them afterward to identify the line of questioning.

- Put people at their ease by asking general background questions at the start, with contentious questions left to the end.

Attorney-Client Issues

Attorneys represent the institution, not the individual employee. Any report should be controlled – sending it into the public domain would waive the attorney-client privilege. Document control includes a statement on each page, numbered copies, and a log of who has received it. All copies should be returned after a set period. Oral presentations may be preferable to written documents.

International Cooperation

International Money Laundering Information Network (IMoLIN) – clearing house of money laundering information, created by the UN, has five features:

- AMLID – anti-money laundering international database, lists laws and regulations per country and contacts for each county. The database is not publically available.
- Reference Data – research, model laws, analysis
- Country Page – links to national FIUs and, full text of AML legislation
- Calendar – training, conferences, seminars, workshops
- Current News

Mutual Legal Assistance Treaties

The first gateway for international cooperation is the MLAT (Mutual Legal Assistance Treaty), a legal basis for transmitting evidence. The following happens:

- A "*commission regatoire*", letter of request, or *letters rogatory* is sent indicating the information requested, the nature of the request and the charges, and the legal basis for the charge.
- The central authority receives this, and sends it to a financial investigator to obtain the information (if possible).
- An investigator from the requesting country visits the country where the information is, and accompanies the local investigator, to obtain the information.
- Permission is then sought from the central authority to remove the evidence back to the requesting country.
- The central authority sends the information to the requesting country, satisfying the request for assistance.
- Local witnesses may need to attend court in the requesting country.

Financial Intelligence Units

The second gateway is the communication between FIUs who receive and analyze STRs. They then pass this information on to law enforcement and other international FIUs. The Egmont Group is the body of FIUs and has over 100 members. 2003 FATF recommendations include specific recommendations as to setting up and running an FIU.

FIUs need to both recognize the international need for FIUs and also work within their local law enforcement and policy framework, set their own priorities, objectives, within their budgets.

FIUs share information internationally using an MOU (Memorandum of Understanding) which allows them to share intelligence (rather than evidence per se).

Key principles from the Egmont group:

- Free exchange of information, on the basis of reciprocity, including spontaneous exchange of information.
- Definitions of offences that differ among jurisdictions should not be a barrier to information exchange.
- Privacy and confidentiality of the data should be assured.
- Information exchange should be informal and rapid, without red tape, or intermediaries.
- Permission to disseminate to law enforcement should be granted, provided it doesn't jeopardize a criminal investigation, is disproportionate to the legitimate interests of a person or company in the providing country, or is not in accordance with national law.

Requesting countries should follow the Egmont principles:

- Submit requests for information as soon as the precise need is identified.
- When an FIU has information that could be useful to another FIU is should be shared immediately.

- Communication should be secure (Egmont Secure Web can use used)
- Use the standard form when requesting information, which includes details of relevant facts.

- Recipients should reply within one week if they have the information, or there is a legal reason why the information can't be provided. If external parties must be consulted (e.g. Banks) then the reply should be within one month, containing all information obtained to date, and an estimate of when it will be completely filled.

The Supervisory Channel

April 2002 "Report on Sharing Information between Jurisdictions in connection with the fight against terrorism" indicates that the supervisory channel is the third gateway. This relates to supervision of financial institutions, and can be used to share general information about financial activity, as well as specific information such as regarding Politically Exposes Persons (PEPs). Information obtained this way should only be used for supervisory purposes, not as evidence, and should not be widely shared with government departments.

Addendum

- SARs do not have any supporting materials attached to them, they are standalone – all materials should be kept separately to enable law enforcement to review them should they wish to, but all information should be on the SAR.
- What is **structuring**? Making cash deposits that are under the reporting threshold. Also known as 'smurfing'.
- What is **refining**? Converting small notes into larger notes.
- The Basel Committee wanted strong KYC to protect the safety and soundness of banks.
- CFAT 19 Recommendations requires that you consider: not limiting the predicate offenses, criminalise conspiracy or association to engage in money laundering, decide whether the predicate offense may have been committed outside the local jurisdiction. It does not suggest that you avoid criminalising money laundering where the offender lacks knowledge of the criminal source of the funds.
- What is **CFT**? Combating the Financing of Terrorism.

Study Questions

Section 1

1. *Which of the following is not an example of layering*
    a) *Using cash deposited in a bank account to purchase an asset*
    b) *Exchanging cash for a monetary instrument*
    c) *Using an inbound wire transfer to purchase an asset*
    d) *Using an inbound wire transfer to purchase a monetary instrument*

2. *What are key effects of money laundering on countries? Choose three.*
    a) *Reputation risk*
    b) *Losing control of regulatory policy*
    c) *Being forced into adverse fiscal policies*
    d) *Losing control of monetary policy*

3. *Risks of correspondent banking include the following. Choose three.*
    a) *The effectiveness of the regulatory regime may be unknown*
    b) *The ultimate customers are at arm's length*
    c) *The USA Patriot Act did not address correspondent banking risks*
    d) *The volumes of transactions are high*

4. *Which of the following are most vulnerable to the placement stage of money laundering? Choose two.*
    a) *Purchasing diamonds*
    b) *Overpaying a credit card balance*
    c) *Obtaining cashiers cheques*
    d) *Internet casinos*

5. *Which of the following describes a payable through account?*
    a) *A numbered account where the customer is unknown*
    b) *A correspondent account that can be used directly by the respondent's customers without the respondent's oversight*
    c) *Internal bank accounts used to assist in the settlement and processing of customer transactions. Also known as omnibus, settlement, or collection account.*
    d) *A system where a bank offers accounts to another bank to enable it to perform transactions in a location where it does not have a physical presence*

6. *What is a risk of concentration accounts?*
    a) *The underlying customer identification can be lost*
    b) *Comingling of clean and dirty funds can occur*
    c) *Customers may be unaware they are using them*
    d) *Confidentiality and secrecy between client and banker*

7. *What are two risks associated with private banking?*
    a) *The area was not covered by the Wolfsburg group*
    b) *Politically exposed persons*
    c) *Private investment companies*
    d) *Lack of competition*

8. *Which of the following is a correct statement?*
    a) *Smurfs travel from bank to bank withdrawing cash from ATMs*
    b) *Smurfing is a way to avoid triggering a currency reporting threshold*
    c) *Smurfs are dead people whose accounts have been taken over by money launderers*
    d) *Smurfing requires an insider at a financial institution*

9. *Which one of the following might indicate microstructuring?*
    a) *Converting $800 of travellers cheques to a wire transfer*
    b) *Using counter deposit slips*
    c) *Large cash deposits*
    d) *Using cash to purchase a gold ingot*

10. *Cuckoo smurfing features which three of the following?*
    a. *An unwitting bank account owner*
    b. *An insider in a financial institution*
    c. *An accomplice in a foreign country who deposits cash*
    d. *Concentration of funds*

11. *What is the best way to guard against the risk of money laundering by bank staff?*
    a. *Ensure that key staff are registered with the regulator*
    b. *Ensure segregation of duties for all tasks*
    c. *Conduct initial and ongoing criminal background checks*
    d. *Ensure managers review staff work periodically*

12. *Why are credit unions (building societies) vulnerable to money laundering?*
    a. *They are small in size*
    b. *They have high levels of cash transactions*
    c. *They offer complex products*
    d. *They are not regulated*

13. *At which stages of money laundering are credit cards used? Choose two.*
    a. *Layering*
    b. *Structuring*
    c. *Integration*
    d. *Placement*

14. *Which of the following are money laundering risks at insurance companies? Choose two:*
    a. *Early cancellation capabilities of car insurance*
    b. *Salesmen are incentivised*
    c. *Underpaying insurance and requesting refunds*
    d. *Cancelling life policies during the 'free look' period*

15. *What is wash trading?*
    a. *The ability to launder funds using nominee accounts*
    b. *The inherent anonymity granted by many broker-dealers*
    c. *The use of offsetting trades to launder funds*
    d. *The trading of commodities*

16. *Securities dealers are attractive to money launderers for the following reasons. Choose three:*
    a. *They have information that can be used for insider trading*
    b. *They use high speed wire transfers*
    c. *They have a competitive, commission-driven culture*
    d. *They use cash accounts that are not subject to banking AML controls*

17. *Casinos and other gaming venues are attractive to money launderers for the following reasons. Choose three:*
    a. *They offer a plausible source of recently acquired wealth*
    b. *Gambles can be placed so that there is very little risk to capital*
    c. *The variety of gambling opportunities are useful at the integration stage*
    d. *Funds can be made available in different jurisdictions*

18. *Which two of the following makes gold the most attractive to money launderers?*
    a. *It has high demand due to religious or cultural reasons*
    b. *It can be used in the placement phase*
    c. *It can be easily melted down*
    d. *It can be used in the layering phase*

19. *Why are travel agents vulnerable to money launderers? Choose one.*
    a. *They sell hotel rooms in high risk destinations*
    b. *Hotels are frequented by politically exposed persons*
    c. *Refunds can be made to third parties*
    d. *They are listed in the FATF 40 recommendations*

20. *Vehicle sellers are susceptible to money laundering because of the following reasons. Choose three:*
    a. *They allow third party payments*
    b. *They sell high value items*
    c. *They allow down trading*
    d. *They allow partial down payments*

21. *Lawyers are more useful in money laundering than company formation agents because of the following reason:*
    a. *They have a client-attorney privilege*
    b. *They can represent the launderer in court*
    c. *They can create complex vehicles such as private investment companies*
    d. *They can act as nominee shareholders, directors and secretaries*

22. *Real estate is most often associated with which two of the following:*
    a. *Layering*
    b. *Placement*
    c. *Integration*
    d. *Structuring*

23. *Under valuing exports are used to:*
    a. *Move money using nominee accounts*
    b. *Enable the black market peso exchange*
    c. *Create fraudulent transfer pricing schemes*
    d. *Add an air of legitimacy to letters of credit*

24. *What three features of prepaid cards make them most attractive to money launderers:*
    a. *Anonymity*
    b. *Widely accepted at merchants*
    c. *High value limits*
    d. *ATM access*

25. *Front companies are useful to the launderer for the following three reasons:*
    a. *They generate legitimate cash which can be comingled with dirty money*
    b. *They provide a source of employment*
    c. *They have low overheads*
    d. *They can be sold for high profits*

26. *Why would a money launderer purchase a company that he already owned?*
    a. *To avoid tax*
    b. *To hide money*
    c. *To repatriate wealth*
    d. *To appear successful*

27. *What is double invoicing?*
    a. *The raising of two invoices payable by the same party against the same goods*
    b. *The raising of two invoices payable by different parties against the same goods*
    c. *A subsidiary purchasing goods from a parent at too high a price*
    d. *The creation of an invoice where the goods are non-existent*

28. *What is a settlor?*
    a. *A beneficiary of a trust*
    b. *A lawyer*
    c. *A third party*
    d. *A person who sets up a trust*

29. *What should banks do in order to mitigate the risk of companies with bearer shares? Choose one.*
    a. *Refuse to do business with such firms*
    b. *Insist that the shares are handed over to the bank for safe keeping*
    c. *Inspect the register of owners*
    d. *Enquire as to the beneficial owners of the company*

30. *What are the main differences between terrorist financing and money laundering?*
    a. *Only one of these is covered by the Wolfsburg group*
    b. *Terrorist financing can involve the use of legitimate funds*
    c. *Layering is used in money laundering, not terrorist financing*
    d. *All of the above*

31. *Which of the following statements is true?*
    a. *An alternative remittance system is usually more expensive than a bank transfer*

b. *Informal value transfer systems settle balances through the normal process of trade*
c. *Hawala is illegal*
d. *Informal remittance systems are only used in the placement phase of money laundering*

32. *How can charities ensure they are less attractive to money launderers? Choose three.*
    a. *Ensure strict oversight and regulation*
    b. *Use standard bank accounts*
    c. *Use full accounting for all expenditure*
    d. *Conduct field audits*

Section 2

33. *Which of the following compliance criteria is not a requirement for membership of FATF?*
    a. *Freezing and confiscation of funds*
    b. *Payment of FATF penalties*
    c. *Customer due diligence*
    d. *International cooperation*

34. *What are the three objectives of FATF?*
    a. *Monitoring implementation of recommendations by members*
    b. *Promoting AML messages worldwide*
    c. *Encouraging the use of risk based methods*
    d. *Monitoring money laundering trends and countermeasures*

35. *What three of the following items did the 2003 revision to the FATF recommendations include:*
    a. *Transparency of legal persons*
    b. *Terrorist financing*
    c. *Predicate offences for money laundering*
    d. *Prohibition of shell banks*

36. *What three of the following items did the 2012 revision to the FATF recommendations include:*
    a. *Merging the 9 terrorist financing recommendations*
    b. *Domestic politically exposed persons*
    c. *Setting up financial intelligence units*
    d. *Tax crimes*

37. *Why does FATF recommend a risk-based approach*
    a. *More effective use of resources*
    b. *More cost effective approach*
    c. *Because FATF better understands risk*
    d. *All of the above*

38. *In what situations does FATF recommend heightened customer due diligence? Choose three:*
    a. *Wire transfers*
    b. *Politically exposed persons*
    c. *New technologies*
    d. *Counter transactions*

39. *FATF recommendations specify which of the following would encounter a FATF designated threshold of €15,000:*
    a. *Bank customers carrying out regular cash transactions*
    b. *Internet casinos*
    c. *Cash dealers of precious stones*
    d. *Car dealers*

40. *Non-Cooperative Countries are measured by the FATF using which criteria? Choose three:*
    a. *Loopholes in financial regulations*
    b. *Obstacles raised by regulatory requirements*
    c. *Inadequate AML resources*
    d. *Geographic location*

41. *Which of the following industries does the FATF guidelines not cover:*
    a. *Notaries*
    b. *Legal professionals*
    c. *Trust and company service providers*
    d. *High value vehicle sales*

42. *According to the Basel paper published in 2001 covering Customer Due Diligence for Banks, what are the four key elements of KYC?*
    a. *Identification, transaction profile, monitoring, reporting*
    b. *Risk management, identification, monitoring, acceptance*
    c. *Risk-based controls, identification, monitoring, acceptance*
    d. *Identification, transaction profile, source of funds, monitoring*

43. *What did the Basel paper published in 1997 covering Core Principles for Effective Banking Supervision, recommend?*
    a. *Strong KYC, high ethical standards, adoption of the FATF recommendations*
    b. *Capital requirements, liquidity measures, monitoring and reporting requirements*
    c. *Controls over private banking, correspondent banking, payable through accounts, and shell banks*
    d. *None of the above*

44. *What did the EU First Directive on Money Laundering (91/308/EEC) cover?*
    a. *Terrorist financing*
    b. *Drug Trafficking*
    c. *International financial services*
    d. *All of the above*

45. *What was not introduced into the scope of the EU Second Directive on Money Laundering (2001/97/EEC)?*
    a. *Politically exposed persons (PEPs)*
    b. *Wilful blindness*
    c. *Precise definition of laundering*
    d. *Bureaux de change and money transmitters*

46. *What was introduced into the scope of the EU Third Directive on Money Laundering (2001/97/EEC)? Choose three.*
    a. *Protection for employees reporting suspicious transactions*
    b. *Collection of statistics on suspicious transactions*
    c. *Life insurance intermediaries*
    d. *Fraud and other serious predicate crimes*

47. *Which regional FATF body was created by a inter-governmental treaty?*
    a. *MONEYVAL (Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures*
    b. *Eurasian Group (EAG)*
    c. *Financial Action Task Force of South America against Money Laundering (GAFISUD – Grupo de Acción Financiera de Sudamérica)*
    d. *Middle East and North African Financial Action Task Force (MENAFATF)*

48. *Which countries are co-operating nations of the Caribbean Financial Action Task Force (CFATF)?*
    a. *Nauru, Aruba, Bahamas*
    b. *UK, USA, Canada, Mexico, France, Spain, the Netherlands*
    c. *Cayman Islands, Guernsey, Seychelles*
    d. *Monaco, Luxembourg, Cyprus*

49. *Which of the following activities is carried out by the Egmont group:*
    a. *Drafting model anti-money laundering laws*
    b. *Promoting the establishment of financial intelligence units*
    c. *Recommends controls within private banking*
    d. *Partnership with Transparency International*

50. Which three of the following did the Wolfsburg group cover:

- *a. Standards and policies for KYC, AML and terrorist financing*
- *b. Prohibition of concentration accounts*
- *c. Enhanced customer due diligence for money services businesses*
- *d. Supporting regulators, judges, prosecutors, financial intelligence units and law enforcement*

51. What does section 311 of the USA Patriot Act cover:

- *a. The ability to designate a foreign jurisdiction, a foreign financial institution, a type of international transaction, or a type of account as a specific concern to be addressed by US banks.*
- *b. Prohibiting correspondent accounts for shell banks*
- *c. Making correspondent account records available within 120 hours*
- *d. Due diligence for non-US private bank customers*

52. What does section 312 of the USA Patriot Act cover:

- *a. The ability to designate a foreign jurisdiction, a foreign financial institution, a type of international transaction, or a type of account as a specific concern to be addressed by US banks.*
- *b. Prohibiting correspondent accounts for shell banks*
- *c. Making correspondent account records available within 120 hours*
- *d. Due diligence for non-US private bank customers*

53. *What does section 313 of the USA Patriot Act cover:*
    a. *The ability to designate a foreign jurisdiction, a foreign financial institution, a type of international transaction, or a type of account as a specific concern to be addressed by US banks.*
    b. *Prohibiting correspondent accounts for shell banks*
    c. *Making correspondent account records available within 120 hours*
    d. *Due diligence for non-US private bank customers*

54. *What does section 319b of the USA Patriot Act cover:*
    a. *The ability to designate a foreign jurisdiction, a foreign financial institution, a type of international transaction, or a type of account as a specific concern to be addressed by US banks.*
    b. *Prohibiting correspondent accounts for shell banks*
    c. *Making correspondent account records available within 120 hours*
    d. *Due diligence for non-US private bank customers*

55. *Which three sentences describe the Office of Foreign Assets Control (OFAC):*
    a. *Enforces economic and trade sanctions*
    b. *Enforces fiscal policy*
    c. *Applies to all US citizens, regardless of location*
    d. *Applies to all US-incorporated entities, including foreign branches*

Section 3

56. *Which of the following statements is correct?*
    a. *AML functions should be centralised to ensure efficiency*
    b. *AML functions should be decentralised to ensure product knowledge*
    c. *AML functions should have a centralised aspect to ensure consistency*
    d. *AML functions should be external to the firm to provide objectivity*

57. *Which three statements describe the motivations behind risk-based approaches to AML?*
    a. *They are flexible to meet the risks of different geographical areas, products, and customers*
    b. *They are effective, as companies know better than regulators how to mitigate risk*
    c. *They are cost-effective, because organisations only need to look at the highest risks*
    d. *They are proportionate, and allow an intelligent, rather than a checkbox, approach*

58. *Which of the following types of companies pose a high risk of money laundering? Choose three:*
    a. *Art dealers, and dealers in precious stones and metals*
    b. *Restaurants, parking, car washes*
    c. *Travel Agencies, machine parts*
    d. *Electronics merchants, supermarkets.*

59. *Which group of banking products is the highest risk:*
    a. *Deposit taking, retail brokerage, cash advances on a credit card*
    b. *Wire transfers, travellers cheques, bankers cheques*
    c. *Foreign exchange, savings accounts, checking accounts*
    d. *Private banking, fixed income bonds, domestic accounts*

60. *What are the four key elements of an AML program? Choose one answer:*
    a. *AML certifications; regulator liaison; law enforcement liaison; and documentation standards*
    b. *Policies & procedures; senior management sponsorship; on-going compliance testing; and third party oversight*
    c. *On-going employee training; designated compliance office ,internal audit testing; and policies, procedures and controls*
    d. *Board approval; approved procedures; supervisor testing; and agreed reporting arrangements*

61. *What should be addressed within the AML policies and procedures?*
    a. *Risk based due diligence*
    b. *Segregation of duties*
    c. *Record keeping requirements*
    d. *All of the above*

62. *Which two are important functions of the designated compliance officer?*
    a. *Creating training*
    b. *Delivering training*
    c. *Staying current with regulatory and legal changes*
    d. *Conducting reviews of AML compliance*

63. *Which of the following is not a requirement for customer due diligence:*
    a. *Profiles of expected account activity*
    b. *Documenting findings*
    c. *Conducting investigations into the source of a client's wealth*
    d. *Investigating unusual activity*

64. *Basel 2003 account opening guidelines included which three of the following items:*
    a. *Government issued unique identification*
    b. *Date and place of birth*
    c. *Occupation, position, employer*
    d. *Countries visited and visas recorded in passport*

65. *Why are politically exposed persons (PEPs) difficult to identify for a retail bank?*
    a. *The large volume of transactions makes screening impractical*
    b. *The lack of identifying information (e.g. date of birth) makes false hits common*
    c. *The lack of PEP name lists make automation impossible*
    d. *The secrecy laws of some jurisdictions means identifying PEPs is impractical*

66. *FDIC guidance issued in 2005 recommended which of the following for 'know your employee' programmes*
    a. *Re-screen when a person is promoted*
    b. *Subject contractors to the same controls*
    c. *Background screen on employment for criminal history*
    d. *All of the above*

67. *Which three of the following would be a red flag in a customer situation:*
    a. *Customers who move frequently*
    b. *International use of ATMs*
    c. *Customers who send wire transfers*
    d. *Turning down high interest rates*

68. *Which three of the following would be a red flag when dealing with cash transactions?*
    a. *Changing large bills for smaller bills frequently*
    b. *Deposits contains lots of fake bills, or very dirty or musty bills*
    c. *Making large deposits without counting the cash*
    d. *Making deposits of currency wrapped in currency straps*

69. *Which three of the following would be a red flag regarding non-cash deposits?*
    a. *Depositing consecutively numbered travellers cheques*
    b. *Depositing bearer bonds*
    c. *Depositing third party cheques*
    d. *Frequent purchase of monetary instruments*

70. *Which three of the following would be a red flag regarding trade finance?*
    a. *Changes to the beneficiary of a letter of credit just before a payment is made*
    b. *Letter of credit is for goods not in demand in the exporting country*
    c. *Goods for import or export are at prices above or below normal market rates*
    d. *Commodities shipped through locations without apparent economic or logistical reason*

71. *Which three of the following would be a red flag regarding employees?*
    a. *Employees carry over vacation days from one year to the next*
    b. *Employee is involved in an large number of unresolved exceptions*
    c. *Employee leads a lavish lifestyle, not in line with the salary*
    d. *Employee circumvents policies*

72. *Which three of the following would be a red flag in an insurance situation?*
    a. *Changes to the beneficiary of car insurance*
    b. *Early redemption of life policy*
    c. *Unconcerned with early redemption charges*
    d. *Cash payments*

73. *Electronic AML solutions offer which three of the following benefits:*
    a. *Monitoring of transactions for signs of laundering*
    b. *Screening of data against known watch lists*
    c. *Efficiencies permitting the outsourcing of compliance functions*
    d. *Automated regulatory reporting*

Section 4

74. *What does a subpoena allow?*
    a. *Entry of a specific location to seize specific categories of documents or items*
    b. *Law enforcement to obtain documents and testimony*
    c. *Law enforcement to commence proceedings*
    d. *Law enforcement to evaluate documents under client-attorney privilege*

75. *What does a search warrant allow?*
    a. *The interview of subjects*
    b. *Entry of a specific location to seize specific categories of documents or items*
    c. *The arrest of a suspect*
    d. *A court case to proceed*

76. *Which three of the following are steps that law enforcement should take when performing an investigation? Choose three.*
    a. *Documenting activity and transactions; reviewing databases; and reviewing licensing and registration files*
    b. *Analysing financial transactions; Reviewing STRs; and conducting computer based searches*
    c. *Decide whether to prosecute; obtain evidence; cross-examine witnesses*
    d. *Follow the money; identify the unlawful activity; and obtain international co-operation*

77. *What three steps should an institution take to respond to all law enforcement investigations?*
    a. *Respond quickly and completely to all requests*
    b. *Narrow overly broad requests*
    c. *Establish a single point of contact*

d. *Notify the customer*

78. *When law-enforcement exercise search warrants, what three things should the organisation do?*
    a. *Ask for the affidavit*
    b. *Ask for the subpoena*
    c. *Ask for the inventory*
    d. *Ask for the warrant*

79. *When should you freeze accounts or assets?*
    a. *When asked to do so by law enforcement*
    b. *Upon receipt of the warrant issued by the court ordering the freeze*
    c. *Upon request of legal counsel*
    d. *All of the above*

80. *Why should 'no comment' be provided to the press when the facts are against an organisation under investigation?*
    a. *To prevent appearing foolish should subsequent leaks occur*
    b. *Because any admission of wrong doing would cause the share price to drop*
    c. *Because any inaccuracies could lead to an investigation by the SEC*
    d. *All of the above*

81. *When should you conduct an internal investigation?*
    a. *When you receive an adverse regulatory opinion*
    b. *When you receive an adverse internal audit report*
    c. *When you receive an employee hotline tip off*
    d. *All of the above*

82. *Which one of the following statement is correct:*
    a. *Documents can be destroyed in line with the document destruction policy even though they may be of use in an on-going government investigation*
    b. *Documents cannot be destroyed in line with the document retention policy*
    c. *Documents can be destroyed in line with the document destruction policy, provided no government investigation is on-going*
    d. *Documents should be retained for a minimum of 6 years*

83. *Which three of the following are useful techniques to use when interviewing employees:*
    a. *Carry out the interview as soon as possible to ensure memories are fresh*
    b. *Interrogation rooms should be set up with bright lights facing the interviewee*
    c. *General background questions should be asked at the start, with contentious questions left to the end*
    d. *Counsel should prepare staff before the interview, and debrief them afterwards to identify the line of questioning.*

84. *What is the main purpose of IMoLIN, International Money Laundering Information Network*
    a. *It created and disseminated model laws*
    b. *It was created by the UN (United Nations)*
    c. *It acts as a clearing house of money laundering information*
    d. *All of the above*

85. *What is a 'commission rogatoire'?*
    a. *A letter requesting cooperation from a foreign central authority*
    b. *A gateway for international cooperation*
    c. *Permission from a central authority that allows a foreign investigation to occur*
    d. *A letter of decline, where a central authority refuses a foreign investigation*

86. *How do FIUs (financial intelligence units) share information internationally?*
    a. *Using a commission rogatoire*
    b. *Using a multilateral legal assistance treaty (MLAT)*
    c. *Using a memorandum of understanding*
    d. *Using the Wolfsburg principles*

87. *What are the principles from the Egmont group related to information sharing? Choose three.*
    a. *Free exchange of information, on the basis of reciprocity*
    b. *Grant permission to law enforcement, if appropriate*
    c. *Respect privacy and confidentiality*
    d. *Share information with every member as a matter of course*

88. *According to the 2002 Basel committee "Report on sharing information between jurisdictions in connection with the fight against terrorism" which of the following statements is true:*
    a. *Supervisors should disseminate information to government departments*
    b. *Information can be used as evidence*
    c. *General information about financial activity can be shared between regulators*
    d. *Specific information about politically exposed persons can be shared between regulators and used as evidence*

Answer Sheet

1		31		61		91	
2		32		62		92	
3		33		63		93	
4		34		64		94	
5		35		65		95	
6		36		66		96	
7		37		67		97	
8		38		68		98	
9		39		69		99	
10		40		70		100	
11		41		71		101	
12		42		72		102	
13		43		73		103	
14		44		74		104	
15		45		75		105	
16		46		76		106	
17		47		77		107	
18		48		78		108	
19		49		79		109	
20		50		80		110	
21		51		81		111	
22		52		82		112	
23		53		83		113	
24		54		84		114	
25		55		85		115	
26		56		86		116	
27		57		87		117	
28		58		88		118	
29		59		89		119	
30		60		90		120	

Answers

1	*Answer B. This answer uses physical cash to purchase an asset, and is a feature of placement. All other answers use money that is already in the financial system and are thus examples of layering*
2	*Answer: A, C, D. Counties can suffer reputational risk if they are known as a haven for money laundering, they may be forced to make adverse fiscal (tax and budget) policy to compensate for the tax revenue lost to criminal laundering, and they may lose control of monetary policy as currency flows are directed by launderers out of the country. The country should use regulatory policy to enforce antimony laundering.*
3	*Answer: A, B, D. While the regulatory regime may be known, the effectiveness of that regime on any one institution may be difficult to assess beyond standard checklists. The arms-length nature of correspondent banking means that customer due diligence of the ultimate customer is difficult or impossible, and the transaction volumes are high, so suspicious transactions are hidden in the noise. The USA Patriot act contained specific provisions concerning correspondent banking in sections 312, 313, 319a & b*
4	*Answer A & C. Gem stones and cashiers cheques can be purchased using cash, making them vulnerable to placement. Credit cards and internet casinos do not usually allow cash payments, and so are less likely to be used as part of the placement phase.*
5	*Answer B. C describes a concentration account, D is a correspondent account, A is numbered account*

6	*Answer A – the internal accounts used by the bank may be set up so that the audit trail is lost when they are used. The other answers are not relevant risks to the use of concentration accounts*
7	*Answer B&C. Politically exposed persons (PEPs) use private banking, and may have access to funds derived from embezzlement or bribes. Wealthy users of private banking often use private investment companies (PICs) to manage their wealth which may hide the beneficial owners. The Wolfsburg group did cover private banking, and there is intense competition in private banking, making those answers incorrect.*
8	*Answer B. Smurfing is used to deposit cash at a financial institution below the reporting threshold. A is incorrect because smurfs deposit cash, rather than withdrawing it. C is incorrect, smurfs often use accounts set up using dead peoples identities, but the term does not refer to them. D is incorrect because this is relates to cuckoo smurfing*
9	*Answer B. Microstructuers often use counter deposit slips as they make many small cash deposits and will have insufficient pre-printed paying in slips. A is incorrect as there is no cash involved, C&D both mention either large cash amounts, or expensive items which would not indicate microstructuring, which uses small amounts of cash, typically under $1000.*
10	*Answer A,B,C. Although the remitter is expecting funds to be sent via an international wire transfer, in a cuckoo smurfing situation, an accompanied in a financial institution diverts it elsewhere. The funds are instead deposited as dirty cash by an accomplice in a foreign country into the unwitting recipient's bank account. There is no concentration of funds as this would cause a discrepancy between the remittance and receipt which would raise the alarm.*

11	*Answer C. All of these are methods to guard against money laundering risks, however not all of them are effective. Registering staff with the regulator is not possible in all jurisdictions, and may only cover senior roles not all roles that might be at risk of money laundering, segregation of duties is effective, but would not be practical for all tasks, reviewing work periodically may be effective, but would very much depend on the depth and scope of the review. The most effective method is to conduct initial and ongoing criminal background checks.*
12	*Answer: B. These financial institutions are low risk because they are small, but they are vulnerable because of the level of cash transactions. They do not usually offer complex products, and they are regulated.*
13	*Answer: A&C. Structuring and placement are methods of disposing of cash, which many credit cards do not permit. They are used for structuring and integration.*
14	*Answer: B&D. Salesmen that are incentivised may overlook their suspicions, and cancelling life insurance during the free look period enables the launderer to obtain a refund of clean money. Underpaying insurance does not lead to an excess cash balance and cancelling car insurance early would not lead to a large refund so is not a significant risk of money laundering.*
15	*Answer: C. The use of two offsetting trades means that the market can move in either direction and the principle is safe. The loss of dirty money in one account is compensated by the creation of legitimate gains in another trading account. None of the other descriptions matches that of a wash trade.*
16	*Answer: B, C, D. Broker dealers are not party to insider information. They do use wire transfers, which are useful to money launderers, the commission driven culture could cause sales staff to overlook the source of funds, and their cash accounts are not subject to the same level of AML oversight at banking accounts.*

17	*Answer: A, B, D. Answer C is incorrect because gaming venues offer a means to place cash, rather than integrate it. All of the other answers are correct.*
18	*Answer: B & D. Gold can be purchased with dirty cash, meaning it is useful in the placement phase. It can also be exchanged for cash or other items or physically handed to another person with little or no audit trail, making it useful in the layering phase. Although gold is in high demand and can be easily melted down, these are not the most useful features of gold to money launderers.*
19	*Answer: C. Expensive flights and hotels can be purchased for a third party, who can then request a refund of the cost.*
20	*Answer: A, C, D. They allow third party payments which can obscure the link between the asset and the source of the funds. They do sell high value items, but this in and of itself does not make the vehicle seller susceptible, so this is not a correct answer. They do allow down trading, with the difference available as a cheque made out from the dealer. They allow partial down payments which could be used for structuring.*
21	*Answer: A The attorney-client privilege means that some information cannot be released to law enforcement. While a lawyer does represent a client in court, this is not part of the money laundering process. Both lawyers and company formation agents can create complex vehicles and act as nominee, so these factors do not make lawyers more useful.*
22	*Answer: A&C. Property is often used to disguise the source of funds, making it useful in the layering phase. It can also be used in the integration phase where an asset such as a holiday complex can be purchased, adding to the air of legitimacy. Because real estate is costly, it is not usually a good candidate for placement, which would require very large sums of cash, or structuring, which requires multiple small sums of cash to avoid reporting thresholds.*

23	*Answer: C. Fraudulent transfer pricing schemes are most often associated with the undervaluing of exports. They can be used in conjunction with the black market peso exchange; however they are not necessary for the BMPE to work. They are not used to move money using nominee accounts. Letters of credit can be used to add an air of legitimacy to undervalued exports, but not the other way around.*
24	*Answer: A, C, D. The ability to use the cards at a wide range of merchants is a benefit to a normal retail customer more than it is a benefit to a money launderer. The global ATM access allows the transfer of money out of the country, the high value limits make them useful as an alternative to smuggling cash, and the anonymity reduced the audit trail that can be linked to the launderer.*
25	*Answer: A,B, D. C is incorrect because although criminally controlled front companies do have lower overheads (as they are not subject to commercial pressures such as bank financing costs) these commercial considerations are not the primary reason the enterprise is used by the launderer. The generation of cash with which to comingle funds is a key driver, as is the need to have legitimate employment to avoid suspicion. The high profits that they generate when sold, due to their artificially high turnover, is another attraction.*
26	*Answer: C. The money launderer uses offshore wealth to purchase the company that he already owns, thus repatriating the cash and maintaining his ownership of the company.*
27	*Answer: C. Double invoicing is where a subsidiary purchases goods from a parent at too high a price, or a parent purchases from a subsidiary at too low a price.*

28	*Answer: D. A settlor is the person who creates the trust which defines how the assets of the trust are to be distributed to the beneficiaries. The settlor may be a lawyer, or other legal professional a third party, or even the beneficiary of a trust, however this is not required.*
29	*Answer: D. There is no requirement to refuse to do business with such entitles, however there is no register of owners to check. The bank cannot insist that the shares be handed over, as possession equates to ownership. The bank should satisfy itself as to the beneficial owners of the entity.*
30	*Answer B. Terrorist financing can involve the use of legitimate funds for illegitimate purposes. The Wolfsburg group included terrorist financing in the 2002 revisions. Layering is used by both money launderers and terrorist financers to disguise the source of funds.*
31	*Answer: B, alternative remittance systems usually settle their balances in the normal process of international trade. Hawala is illegal in most, but not all, countries, alternative remittance systems are usually less expensive than bank transfers, and these systems can be used in any phase of money laundering, not just the placement phase.*
32	*Answer: B, C, D. Charities are not subject to strict oversight or regulation, so this would not be possible. The charity can ensure that normal bank accounts are used, so that bank AML controls are in place. Accounting for all expenditure ensures a clear audit trail, and field audits can ensure that expenditure is appropriate.*
33	*Answer: B. FATF cannot impose fines or apply other direct sanctions.*
34	*Answer: A, B, D. Although FATF does recommend risk based measures in its guidance; it's not a specific stated objective.*
35	*Answer: B, C, D. The transparency of legal persons was already in the original FATF recommendations*

36	*Answer: A, B, D. Setting up an FIU was a function of the IMF and World Bank, further codified by the Egmont Group.*
37	*Answer: A. It is recognised that a budget will always be limited, and the risk based approached allows the best use of this budget. The motivation is not to save costs, or for the FATF to specify the risks faced by a specific institution or jurisdiction.*
38	*Answer: A, B, C. Counter transactions should be subject to currency reporting thresholds and suspicious transaction reporting, but not enhanced customer due diligence.*
39	*Answer: C. Dealers of precious metals and stones are subject to a $/€15,000 threshold for reporting when dealing in cash. The same threshold also applies to financial institutions, but only for occasional customer transactions. Internet casinos are subject to a $/€3,000 limit. Car dealers are not covered by the reporting thresholds.*
40	*Answer: A, B, C. The geographic location is not a measure of cooperation.*
41	*Answer: D. The FATF recommendations cover the others in some circumstances (such as when managing client money, or acting as a nominee shareholder)*
42	*Answer B. Although the order has been re-arranged, these are the four key elements of KYC according to the paper.*
43	*Answer: A. The paper covered KYC, the use of high ethical standards in the fight against criminals using the banking system, and urged the adoption of the FATF 40 recommendations.*
44	*Answer: B. The directive only covered drug trafficking and domestic financial services; however, the scope could be broadened by member states to cover other predicate crimes.*
45	*Answer: A. PEPS were introduced in the Third Directive.*
46	*Answer: A, B, C. Fraud and other serious predicate crimes were introduced in the Second Directive.*

47	*Answer: C.The Financial Action Task Force of South America against Money Laundering (GAFISUD – Grupo de Acción Financiera de Sudamérica) was set up by an inter-governmental treaty.*
48	*Answer: B. Nauru, Guernsey, Seychelles, Monaco, Luxembourg and Cyprus are known as tax havens, they are not CFATF co-operating nations*
49	*Answer: B the Egmont group is a body of financial intelligence units (FIUs)*
50	*Answer: A, B, C. The Wolfsburg group is an association of banks and is concerned with managing banking policy, not the link to other enforcement bodies.*
51	*Answer: A is the content of section 311*
52	*Answer: D is the content of section 312*
53	*Answer: B is the content of section 313*
54	*Answer: C is the content of section 319b*
55	*Answer: A, C, D. OFAC is not involved in fiscal (tax and expenditure) matters.*
56	*Answer: C. AML functions can be either centralised or decentralised; however they should ensure that they have a centralised aspect to ensure consistency.*
57	*Answer A, B, D. Although focussing on only high risks could be a cost saving measure, cost effectiveness should not be a primary motivation for the approach*
58	*Answer A, B, C. Electronics merchants and supermarkets are not generally considered to represent a high risk of money laundering*
59	*Answer B. All three of these are high risk as they allow cash management and are negotiable instruments. All of the other answers start with a high risk activity, followed by two activities that are not considered high risk.*

60	*Answer: C. The four key elements of an AML program are internal policies, procedures and controls, with a designated compliance officer with day-to-day oversight of the program. This should be combined with ongoing training and an independent audit function to test the program.*
61	*Answer: D. They should all be addressed within the policies and procedures.*
62	*Answer A & C. The training could be delivered by another competent individual once it has been created by the compliance officer in line with the organisation's needs. Reviews of AML compliance should be carried out by an independent function separate from the compliance officer.*
63	*Answer: C. Although understanding the client's source of wealth should be validated as part of CDD, conducting an investigation without any suspicion is not a requirement.*
64	*Answer: A, B, C. There is no requirement to review the passport for visas and visits.*
65	*Answer: B. The name lists of PEPs do not include date of birth, which means that larger banks are likely to have many matches based on the name alone.*
66	*Answer: D. All of these were recommended by the FDIC*
67	*Answer A, B, D. Sending wire transfers, by itself, is not a red flag.*
68	*Answer B, C, D. Exchanging large bills for smaller bills is common for retail shops that provide change. The others are all red flags.*
69	*Answer A, C, D. Bearer bonds cannot be deposited.*
70	*Answer A, C, D. B would be a red flag if the goods were not in demand in the importing country, but the lack of domestic demand could be a good reason to export.*
71	*Answer B, C, D. Carrying over vacation would only be a red flag if it amounted to not taking periodic vacations at all in order to prevent someone else taking on their responsibilities while they are out of the office, and potentially revealing wrongdoing.*

72	*Answer B, C, D. It is not normally possible to use car insurance as a money laundering vehicle, and changing the beneficiary on a policy is not usually permitted.*
73	*Answer: A, B, D. Outsourcing of compliance is not a stated benefit of electronic AML solutions.*
74	*Answer: B. A subpoena allows law enforcement to obtain documents and testimony. The entry of a specific location requires a search warrant, law enforcement can commence proceedings without a subpoena, and law enforcement cannot generally evaluate documents under privilege.*
75	*Answer B. Interviewing subjects can only happen after arrest and arrest can only occur with an arrest warrant. A court case may come after the search warrant after evidence of criminal wrong-doing is discovered.*
76	*Answer: A, B, D. The points within C would be carried out after the investigation, if criminal wrong-doing was identified*
77	*Answer: A, B, C. The institution should not notify the customer, which would constitute 'tipping off' in many jurisdictions.*
78	*Answer A, C, D. The affidavit accompanies the warrant, and contains additional information. It may not be possible to obtain, but should always be asked for. The inventory of items removed should also be requested. There would not be a subpoena issued at the same time as the search warrant.*
79	*Answer B. Assets may only be frozen upon court order.*
80	*Answer: C. Although the share price may drop, admitting wrong doing during an investigation would be premature, appearing foolish in the light of later leaks is less important than ensuring that true and accurate representations are made to the market.*
81	*Answer: C. The other situations would warrant remediation of the identified issues, but it should not be necessary to conduct an investigation in order to do this.*

82	*Answer: C. Once notified of an investigation, documents should no longer be destroyed, as they may need to be provided as evidence. Documents are normally permitted to be destroyed in line with the destruction policy. Retaining documents for a minimum of 6 years would depend on the specific documentation and the legal requirements of the jurisdiction. It is not a blanket approach to all documents.*
83	*Answer: A, C, D. There is no need to set up bright lights facing interviewees in an interview situation.*
84	*Answer: C. IMoLIN was set up with its main purpose as a clearing house of information. Answers A and B are both correct, but are not the main purpose of the organisation.*
85	*Answer A. It is a letter of request, issued to a foreign authority, seeking their cooperation in an investigation. It forms part of the gateway for Mutual legal assistance treaties to operate, however it is not the gateway itself. It is also does not imply permission being granted or refused.*
86	*Answer: C. A memorandum of understanding MOU) is used by FIUs to share information. A commission rogatoire is used by law enforcement under a MLAT. The FIUs adhere to the Egmont principles to share information, not the Wolfsburg principles.*
87	*Answer: A, B, C. D is incorrect as the information should be shared with every relevant FIU, but not every member as a matter of course.*
88	*Answer: C. Supervisors should not disseminate information to government departments, information may not be used as evidence, and specific information about PEPs can be shared, but not used as evidence.*

CPSIA information can be obtained
at www.ICGtesting.com
Printed in the USA
FFOW02n1439300117
31931FF

Studying for your ACAMS ® CAMS AML exam can be daunting. Anti Money Laundering is a complex subject, and plain-talking information is difficult to find. This book was created to provide some practical, concise and easy-to-understand revision notes. As well as covering all key areas of Anti Money Laundering, the book also covers Prevention of Terrorist Financing.

The book contains an exclusive set of mock practice exam questions, written in a similar style to the actual exam so you will be well prepared for the question style on the day. The 88 question exam covers every aspect of the material so you can address any gaps in your knowledge and re-study the related material.

Every question also includes the correct answer, and a detailed explanation as to why the answer is correct to help you better understand the logic behind the solutions.

P8-AAD-237

ISBN 9781530061662
90000 >
9 781530 061662